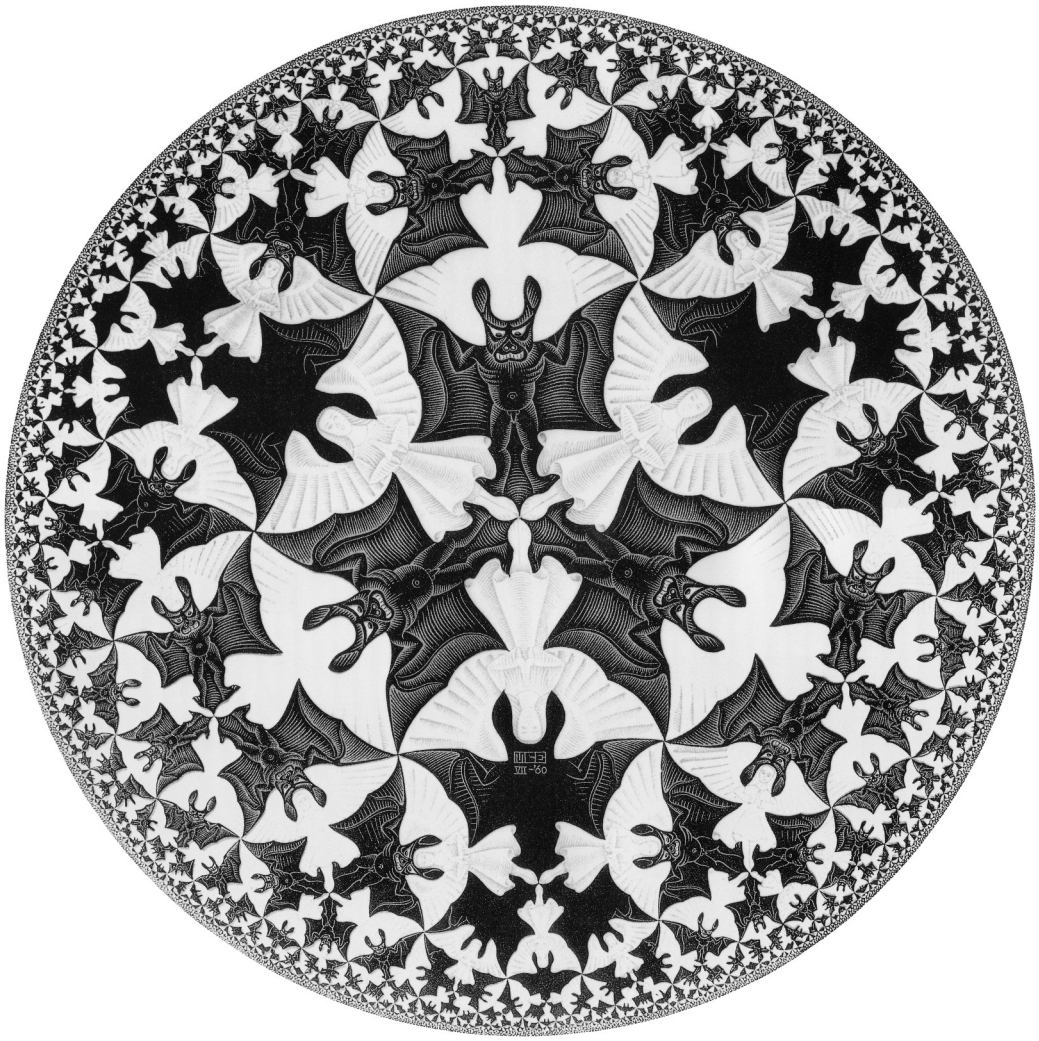
Abstract and Commutative Algebra

Rings, Modules, (Multi-)Linear Algebra, Polynomials,

Spectral Theory, Ring Extensions, Krull-Dimension, ...



by A. B. Zeidler

If you have read this text, I would like to invite you to contribute to it:
Comments, corrections and suggestions are very much appreciated, at *zeidler@math.uni-tuebingen.de*

For the latest version and further readings, visit:



e.pcloud.link/publink/show?code=kZBvhnZEqstjOJc17uS3meyVfAoOSLhRkLk

This book is dedicated to the entire mathematical society:
To all those who contribute to mathematics and keep it alive by teaching it.

思考

Copyright (C) May 7, 2025 (1333 pages)

by Andreas Bernhard Zeidler

This material may be referenced, reproduced and distributed in whole or in part, in any medium physical or electronic, provided that (1) the terms of the *Open Publication License* are adhered to, that (2) this license or an incorporation of it by reference is displayed in the reproduction and that (3) the original author and a reference to the site of this document is clearly stated. I.e. any reproduction or distribution has to meet all the conditions set forth in the *Open Publication License*, v1.0 or later, given in section 0.2 (the latest version is presently available at www.opencontent.org/openpub). Distribution or derivation of the work for commercial purposes is prohibited, unless prior permission is obtained from the copyright holder.

Contents

0 Prelude **7**

0.1 About this Book . . . 7
0.2 Open Publication License . . . 11
0.3 Notation and Symbols . . . 12
0.4 A Primer on Sets . . . 19
0.5 Some Tools from Set Theory . . . 31
0.6 A Primer on Classes . . . 39

1 Groups and Rings **43**

1.1 Defining Groups . . . 43
1.2 Permutations . . . 49
1.3 Defining Rings . . . 56
1.4 Examples . . . 60
1.5 First Concepts . . . 71
1.6 Ideals . . . 78
1.7 Homomorphisms . . . 91
1.8 Ordered Rings . . . 99
1.9 Products . . . 105

2 Commutative Rings **111**

2.1 Maximal Ideals . . . 111
2.2 Prime Ideals . . . 117
2.3 Radical Ideals . . . 122
2.4 Noetherian Rings . . . 129
2.5 Unique Factorisation Domains . . . 137
2.6 Euclidean Domains . . . 149
2.7 Principal Ideal Domains . . . 156
2.8 Lasker-Noether Decomposition . . . 162
2.9 Finite Rings . . . 172
2.10 Localization of Rings . . . 176
2.11 Local Rings . . . 188
2.12 Dedekind Domains . . . 195
2.13 Goldman Domains . . . 201

3 Modules **206**
3.1 Defining Modules . . . 206
3.2 First Concepts . . . 219
3.3 Direct Sums . . . 226
3.4 Ideal-induced Modules . . . 234
3.5 Block Decompositions . . . 240
3.6 Dependence Relations . . . 246
3.7 Linear Dependence . . . 250
3.8 Homomorphisms . . . 257
3.9 Isomorphism Theorems . . . 264
3.10 Rank of Modules . . . 273
3.11 Noetherian Modules . . . 280
3.12 Localization of Modules . . . 291
3.13 Tensor Products . . . 300
3.14 Direct Limits . . . 318

4 Linear Algebra **328**
4.1 Matrix Algebra . . . 328
4.2 Elementary Matrices . . . 343
4.3 Linear Equations . . . 351
4.4 Matrix Representations . . . 365
4.5 Determinants . . . 373
4.6 Rank of Matrices . . . 389
4.7 Duality Theory . . . 401
4.8 Vector Geometry . . . 420
4.9 Linear Optimization . . . 435

5 Structure Theorems **436**
5.1 Primary Decomposition . . . 436
5.2 Invariant Factors . . . 450
5.3 Diagonalization . . . 459
5.4 Normal Forms . . . 474
5.5 Number Fields . . . 478
5.6 Solving linear ODEs . . . 478

6 Functional Analysis **479**
6.1 Metrics and Topologies . . . 479
6.2 Continuous Maps . . . 492
6.3 Banach Spaces . . . 502
6.4 Hilbert Spaces . . . 503
6.5 Operatoralgebras . . . 503

7 Polynomial Rings **504**
7.1 Monomial Orders . . . 505
7.2 Defining Polynomials . . . 511
7.3 The Standard Cases . . . 518
7.4 Graded Algebras . . . 530
7.5 Polynomial Functions . . . 539
7.6 Derivations . . . 552
7.7 Gröbner Bases . . . 555
7.8 Solution Formulae . . . 556
7.9 Irreducibility Tests . . . 560

8 Ring Extensions **561**
8.1 Basic Notions . . . 561
8.2 Transfer of Ideals . . . 569
8.3 Integral Extensions . . . 576
8.4 Algebraic Dependence . . . 585
8.5 Algebraically closed Fields . . . 593
8.6 Galois Theory . . . 611
8.7 Krull Dimension . . . 612
8.8 Spectrum of a Ring . . . 628
8.9 Regular Local Rings . . . 638
8.10 Hilbert-Samuel Polynomial . . . 642

9 Group Theory **643**
9.1 Basic Notions . . . 643
9.2 Group Actions . . . 644
9.3 Some Number Theory . . . 648
9.4 Representation Theory . . . 649

10 Homological Algebra **650**
10.1 Diagram Chasing . . . 651
10.2 Projective Modules . . . 651
10.3 Flat Modules . . . 651
10.4 Homology Modules . . . 651
10.5 Differentials . . . 651

11 Categorial Algebra **652**
11.1 Categories . . . 652
11.2 Functors . . . 665
11.3 Universal Properties . . . 671
11.4 Abelian Categories . . . 675

12 Valuations **676**

13 Symbols **677**

14 List of Proofs **680**

15 All the Proofs **681**

15.1 Proofs of Chapter 0 681
15.2 Proofs of Chapter 1 709
15.3 Proofs of Chapter 2 747
15.4 Proofs of Chapter 3 749
15.5 Proofs of Chapter 4 1013
15.6 Proofs of Chapter 5 1154
15.7 Proofs of Chapter 6 1185
15.8 Proofs of Chapter 7 1208
15.9 Proofs of Chapter 8 1213
15.10 Proofs of Chapter 11 1321

Chapter 0

Prelude

0.1 About this Book

The Aim of this Book

Mathematics knows two directions - analysis and algebra - and any mathematical discipline can be weighted how analytical resp. algebraical it is. Analysis is characterized by having a notion of convergence that allows to approximate solutions (and reach them in the limit). Algebra is characterized by having no notion convergence and hence allowing finite computations only. This book now is meant to be a thorough introduction into algebra.

So where does algebra draw its power from? Many structures can be seen by clever computations - like determinant theory or dimension in vector spaces. But a lot of insights are derived from the order the subset relation "$\subseteq$" establishes on the algebraic object - e.g. maximal ideals are one of the mostly used tools. More generally Zorn's lemma lies at the bottom of so many theorems. And at some points, when finite computations are not enough, algebra has to turn to topology. Analytical arguments (convergence and taking limits) are exceedingly rare, however. In this sense algebra is the more fundamental theory.

Likewise every textbook on mathematics is drawn between two pairs of extremes: (easy understandability versus great generality) and (completeness versus having a clear line of thought). Among these contrary poles we usually chose (generality over understandability) and (completeness over a clear red line). Nevertheless we try to reach understandability by being very precise and accurate and including many remarks and examples.

At last some personal philosophy: A perfect proof is like a perfect gem - unbreakably hard, spotlessly clear, flawlessly cut and beautifully displayed. In this book we are trying to collect such gemstones. And we are proud to claim, that we are honest about where a proof is due and present complete proofs of almost every claim contained herein.

Most textbooks on more advanced topics only present the stepping stones of how a proof works and do not bother to fill in the details. It is commonplace that some propositions are given in exercises only, completely devoid of any proof. While this might be sufficient to get the idea across, we want to raise a question here: How can the reader convince himself, that the proof truly works out, without filling in the details himself? This is why we chose to present *full* proves of *all* propositions and theorems, we do not hesitate to get our hands dirty. This makes this textbook *very* different from almost any other.

This Book is Written for

many different kinds of mathematicians: Primarily it is meant to be a source of reference for intermediate to advanced students, who have already had a first contact with algebra and now closely examine some topic for their seminars, lectures or own thesis. But because of its great generality and completeness it is also suited as an encyclopedia for professors who prepare their lectures and researchers, as a source of reference covering the established theory.

Frankly this book is not perfectly suited to be a monograph for novices to mathematics. So if you are one, we think you can greatly profit from this book, but you will probably have to consult additional monographs (at a more introductory level) to help you guide you through this text.

Prerequisites

We take for granted, that the reader is familiar with the basic notions of naive logic (statements, implication, proof by contradiction, usage of quantifiers, ...). We sketch some naive set theory (Cantor's notion of a set, functions, partially ordered sets, equivalence relations, Zorn's Lemma, ...) but a thorough introduction would have to start with mathematical logic. We will present a short introduction to classes and the NBG axioms, when it comes to category theory. Further we require some basic knowledge of integers (including proofs by induction) and how to express them in decimal numbers. We will sometimes use the field of real numbers, as they are most probably well-known to the reader, but they are not required to understand this text. Aside from these prerequisites we will start from scratch.

Topics Covered

We start by introducing groups and rings, immediately specializing on rings. Of general ring theory we will introduce the basic notions only, e.g. the isomorphism theorems. Then we will turn our attention to commutative rings, which will be the first major topic of this book: We closely study maximal ideals, prime ideals, intersections of such (radical ideals) and the relations to localization. Further we will study rings with chain conditions (noetherian and artinian rings) including the Lasker-Noether theorem. This will lead to standard topics like the fundamental theorem of arithmetic. And we conclude commutative ring theory by studying discrete valuation rings, Dedekind domains and Hilbert rings.

Then we will turn our attention to modules, including rank, dimension and length. We will see that modules are a natural and powerful generalization of ideals and large parts of ring theory generalizes to this setting, e.g. localization and primary decomposition. Module theory naturally leads to linear algebra, i.e. the theory of matrix representations of a homomorphism of modules. Applying the structure theorems of modules (the invariant factor theorem to be precise) we will treat canonical form theory (e.g. rational canonic form and Jordan normal form). Our treatment of the invariant factor theorem is one of the flagships of this text. This part is concluded by presenting a thorough introduction to what is called multi-linear algebra. We will study dual pairings and tensor products of modules (and algebras) over a commutative base ring.

Vector spaces over the reals or complex numbers can be handles even in the case of infinite dimension. Hence there is a natural generalisation of linear algebra over these fields, that is called functional analysis. We will settle with the bounded case however - undbounded operators (that are required in quantum mechanics) would require measure theory and integration theory and this would call for a textbook of its own. So we only aim for the spectral theorem of bounded operators.

Next we will study polynomials from top down: That is we introduce general polynomial rings (also known as group algebras) and graded algebras. Only then we will regard the more classical problems of polynomials in one variable and their solvability. Finally we will regard polynomials in several variables again. Using Gröbner bases it is possible to solve abstract algebraic questions by purely computational means.

This will set the stage for our treatment of ring extensions: We will introduce the concept of integral ring extensions, transcendence bases and the Noeterian normalisation theorem. Another flagship of this text is the treatment of the Krull dimension of a ring. Although we stay purely algebraic we gain our inspiration from algebraic geometry here and include some remarks to enlighten the relation between these fields. Afterwards we turn our attention to systems of parameters, Galois theory and the Hilbert-Samuel polynomial, which provides another way of proving Krull's height theorem.

Then we will return to group theory: Most textbooks begin with this topic, but we chose not to. Even though group theory seems to be elementary and fundamental this is not quite true. In fact it heavily relies on arguments like divisibility and prime decomposition of integers, topics that are native to ring theory. And commutative groups are best treated from the point of view of module theory. Never the less you might as well skip the previous sections and start with group theory right away. We will present the standard topics: The isomorphism theorems, group actions (including the formula of Burnside), the theorems of Sylow and lastly the p-q-theorem. However we are aiming directly for the representation theory of finite groups.

Thus we have gathered a whole bunch of separate theories - and it is time for a second structurization (the first structurization being algebra itself). We will introduce the notions of categories, functors, equivalence of categories, (co-)products and so on. Categories are merely a manner of speaking - nothing that can be done with category theory could not have been achieved without. Yet the language of categories presents a unifying concept for all the different branches of mathematics, extending far beyond algebra. So we will first recollect which part of the theory we have established is what in the categorical setting. The categorial language is the right setting to treat chain complexes, especially exact sequences of modules. Finally we will present the basics of abelian categories as a unifying concept of all those separate theories.

Topics not Covered

There are many instances where, dropping a finiteness condition, one has to introduce some topology in order to pursue the theory further. Examples are: Linear algebra on infinite dimensional vector-spaces, representation theory of infinite groups and Galois theory of infinite field extensions. Another natural extension would be to introduce the Zariski topology on the spectrum of a ring, which would lead to the theory of schemes directly. Yet the scope of this text is purely algebraic and hence we will usually stop at the point where topology sets in (but give hints for further readings).

The Two Parts

Mathematics has a peculiarity to it: There are problems (and answers) that are easy to understand but hard to prove. The most famous example is Fermat's Last Theorem - the statement (for any $n \geq 3$ there are no non-trivial integers $(a, b, c) \in \mathbb{Z}^3$ that satisfy the equation $a^n + b^n = c^n$) can be understood by anyone. Yet the proof is *extremely* hard to provide. Of course this theorem has no value of its own (it is the proof that contains deep insights into the structure of mathematics), but this is no general rule:

E.g. the theorem of Wedderburn (every finite skew-field is a field) is easy and useful, but its proof requires the more advanced method of cyclotomic polynomials. Just a little more advanced: In a noetherian ring R any non-empty set $\mathcal{P} \neq \emptyset$ of prime ideals $\mathcal{P} \subseteq \operatorname{Spec}(R)$ contains both a maximal element $\mathfrak{p}^*$ and a minimal element $\mathfrak{p}_* \in \mathcal{P}$. The proof of the existence of $\mathfrak{p}_*$ requires Krull's height theorem, which is the capstone of dimension theory in commutative rings.
Thus we have chosen an unusual approach: We have separated the truth (i.e. definitions, examples and theorems) from their proofs. This enables us to present the truth in a stringent way, that allows the reader to get a feel for the mathematical objects displayed. Most of the proofs could have been given right away, but in several cases the proof of a statement can only be done after we have developed the theory further. Thus the sequel of theorems may (and will) be different from the order in which they are proved. Hence the two parts.
The easiest way to deal with this is the following: As you probably read the pdf of this text anyway, just open up two copies - one for the theorems and one for the proofs. Then you can easily switch between back and forth from the claim and its proof.

On Names

Many properties are named after famous mathematicians, we speak of noetherian rings and the Krull-dimension. When it comes to naming, we use the following conventions: (1) If the name of a mathematician is used in the name of a concept (a noun), we use a capital letter. We speak of the lemma of Gauss or the Krull-dimension of a ring. (2) If the name of a mathematician is used descriptively (in an adjective or adverb), we use a small letter. Rings are called artinian, or noetherian and $\mathbb{Z}[i]$ are the gaussian integrers. This is *not* an expression of disrespect, quite the contrary. But we feel, that the text gets more pleasant to read, in doing so.

Our best Advice

It is a well-known fact, that some proofs are just computational and only contain little (or even no) insight into the structure of mathematics. Others are brilliant, outstanding insights that are of no lesser importance than the theorem itself. Thus we have already included remarks of how the proof works in the first part of this book. And our best advice is to read a section entirely to get a feel for the objects involved - only then have a look at the proofs that have been recommended. Ignore the other proofs, unless you have to know about them, for some reason. At several occasions this text contains the symbols ($\diamondsuit$) and ($\blacksquare$) . These are meant to guide the reader in the following ways:

($\diamondsuit$) As we have assorted the topics covered thematically (paying little attention to the sequel of proofs) it might happen that a certain example or theorem is far beyond the scope of the theory presented so far. In this case the reader is asked to read over it lightly (or even skip it entirely) and return to it later (after he has gained some more experience).

($\blacksquare$) On some very rare occasions we will append a theorem without giving a proof (if the proof is beyond the scope of this text). Such an instance will be marked by the *black box* symbol. In this case we will always give a complete reference of the most readable proof the author is aware of. And this symbol will be hereditary, that is once we use a theorem that has not been proved any other proof relying on the unproved statement will also be branded by the black box symbol.

0.2 Open Publication License

I. Copyright

The copyright to each Open Publication is owned by its author(s) or designee.

II. Scope of License

The following license terms apply to all Open Publication works, unless otherwise explicitly stated in the document. Mere aggregation of Open Publication works or a portion of an Open Publication work with other works or programs on the same media shall not cause this license to apply to those other works. The aggregate work shall contain a notice specifying the inclusion of the Open Publication material and appropriate copyright notice.

Severability: If any part of this license is found to be unenforceable in any jurisdiction, the remaining portions of the license remain in force.

No Warranty: Open Publication works are licensed and provided "as is" without warranty of any kind, express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose or a warranty of non-infringement.

III. Requirements on both unmodified and modified Versions

Any publication in standard (paper) or any other (e.g. electronic) form shall require the citation of the original publisher and author. The publisher and author's names shall appear on all outer surfaces of the book. On all outer surfaces of the book the original publisher's name shall be as large as the title of the work and cited as possessive with respect to the title.

IV. Requirements on Modified Works

All modified versions of documents covered by this license, including translations, anthologies, compilations and partial documents, must meet the following requirements:

- The modified version must be labeled as such.
- The person making the modifications must be identified and the modifications dated.
- Acknowledgement of the original author and publisher if applicable must be retained according to normal academic citation practices. The location of the original unmodified document must be identified.
- The original author's (or authors') name(s) may not be used to assert or imply endorsement of the resulting document without the original author's (or authors') permission.

V. Good-Practice Recommendations

In addition to the requirements of this license, it is requested from and strongly recommended of re-distributors that:

- If you are distributing Open Publication works on hard-copy or CD-ROM, you provide e-mail notification to the authors of your intent to redistribute at least thirty days before your manuscript or media freeze, to give the authors time to provide updated documents. This notification should describe modifications, if any, made to the document.
- All substantive modifications (including deletions) be either clearly marked up in the document or else described in an attachment to the document. Finally, while it is not mandatory under this license, it is considered good form to offer a free copy of any hard-copy and CD-ROM expression of an Open Publication-licensed work to its author(s).

VI. License Options

Distribution and derivative of the work for commercial purposes is prohibited, unless prior permission is obtained from the copyright holder in written form. The work may be distributed without prior permission from the copyright holder, for purely educational purposes, that are completely free of charge, provided the Good-Practice Recommendations are fulfilled.

0.3 Notation and Symbols

Preliminaries

We now wish to include a set of the frequently used symbols, conventions and notations. We will elaborate on most of the set-theoretic constructions and facts summarized here, in section 0.4.

- First of all we employ the nice convention (introduced by Halmos) to write *iff* as an abbreviation for *if and only if*. That is A iff B is just the same, as $A \iff B$.
- We denote the set of *natural numbers* by $\mathbb{N} := \{ 0, 1, 2, 3, \dots \}$. That is $\mathbb{N}$ are the positive integers including zero. And for any two integers $a, b \in \mathbb{Z}$ we denote the interval of integer numbers ranging from a to b by $a \dots b := \{ k \in \mathbb{Z} \mid a \leq k \leq b \}$.
- We will denote the set of *integers* by $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N})$, and the set of *rational numbers* by $\mathbb{Q}$. Whereas $\mathbb{Z}$ will be taken for granted, the rational numbers will be introduced as the quotient field $\mathbb{Q} = \{ a/b \mid a, b \in \mathbb{Z}, b \neq 0 \}$ of $\mathbb{Z}$ in (1.31) and in section 2.10.
- The *reals* will be denoted by $\mathbb{R}$ and we will present an example of how they can be defined (without proving their properties however). The *complex numbers* will be denoted by $\mathbb{C} = \{ a + ib \mid a, b \in \mathbb{R} \}$ and we will present several ways of constructing them.
- $(\diamondsuit)$ We will sometimes use the *Kronecker-Symbol* $\delta(a, b)$ (in the literature this is also denoted by $\delta_{a,b}$), which is defined to be 1 iff $a = b$ and 0 for any $a \neq b$, formally

$$\delta(a, b) \;=\; \delta_{a,b} \;:=\; \begin{cases} 1 \text{ if } a = b \\ 0 \text{ if } a \neq b \end{cases}$$

 In most cases a and $b \in \mathbb{Z}$ will be integers and 0, $1 \in \mathbb{Z}$ will be integers, too. But in general we are given some ring $(R, +, \cdot)$ and a, $b \in X$ will be elements of an arbitrary set X. Then the elements 0 and $1 \in R$ on the right hand side are taken to be the zero-element 0 and unit-element 1 of the base ring R used.
- We will write $A \subseteq X$ to indicate that A is a subset of X and $A \subset X$ will denote strict inclusion (i.e. $A \subseteq X$ and there is some $x \in X$ with $x \notin A$). For any set X we denote its **power set** (i.e. the set of all its subsets) by $\mathcal{P}(X) := \{ A \mid A \subseteq X \}$. And for a subset $A \subseteq X$ (and X is understood) we denote the **complement** of A in X by $\complement A := X \setminus A$.
- Listing several elements $x_1, \dots, x_n \in X$ of some set X, we do not require these x_i to be pairwise distinct (e.g. $x_1 = x_2$ might well happen). Yet if we only give explicit names x_i to the elements of some previously given subset $A = \{ x_1, \dots, x_n \} \subseteq X$ we already consider the x_i to be pairwise distinct (that is $x_i = x_j$ implies $i = j$). Note that if the x_i (not the set $\{ x_1, \dots, x_n \}$) have been given, then $\{ x_1, \dots, x_n \}$ may hence contain fewer than n elements!
- Given an arbitrary set of sets $\mathcal{A}$ we define the *grand union* $\bigcup \mathcal{A}$ and the *grand intersection* $\bigcap \mathcal{A}$ to be the set consisting of all elements a that are contained in one (resp. all) of the sets $A \in \mathcal{A}$

$$\bigcup \mathcal{A} \;:=\; \{ a \mid \exists\, A \in \mathcal{A} : a \in A \}$$

$$\bigcap \mathcal{A} \;:=\; \{\, a \mid \forall\, A \in \mathcal{A} : a \in A \,\}$$

Note that $\bigcap \mathcal{A}$ only is a well-defined set, if $\mathcal{A} \neq \emptyset$ is non-empty. A well-known special case of this is the following: Consider any two sets A and B and let $\mathcal{A} := \{\, A, B \,\}$. Then $A \cup B = \bigcup \mathcal{A}$ and $A \cap B = \bigcap \mathcal{A}$. This notion is just a generalization of the ordinary union and intersection to arbitrary collections $\mathcal{A}$ of sets.

- If X and Y are any sets then we will denote the set of all functions from X to Y by $\mathcal{F}(X,Y) = Y^X = \{\, f \mid f : X \to Y \,\}$. And for any such function $f : X \to Y : x \mapsto f(x)$ we will denote its **graph** (note that from the set-theoretical point of view f *is* its graph) by

$$\Gamma(f) \;:=\; \{\, (x, f(x)) \mid x \in X \,\} \;\subseteq\; X \times Y$$

- Once we have defined functions, it is easy to define arbitrary **cartesian products**. That is let $I \neq \emptyset$ be any non-empty set and for any $i \in I$ let X_i be another set. Denote the union of all the X_i by

$$X \;:=\; \bigcup_{i \in I} X_i \;=\; \{\, x \mid \exists\, i \in I : x \in X_i \,\}$$

Then the cartesian product of the X_i consists of all the functions $x : I \to X$ such that for any $i \in I$ we have $x_i := x(i) \in X_i$. Note that thereby it is customary to write (x_i) in place of x. Formally

$$\prod_{i \in I} X_i \;:=\; \{\, x : I \to X : i \mapsto x_i \;\mid\; \forall\, i \in I : x_i \in X_i \,\}$$

- If $I \neq \emptyset$ is any index set and $A_i \subseteq X$ is a non-empty subset of X (where $i \in I$) then the **axiom of choice** states that there is a function $a : I \to X$ such that for any $i \in I$ we get $a(i) \in A_i$. In other words the product of non-empty sets is non-empty again. It is a remarkable fact that this seemingly trivial property has far-flung consequences, the lemma of Zorn being the most remarkable one.

$$\prod_{i \in I} X_i \;\neq\; \emptyset \quad\Longleftrightarrow\quad \forall\; i \in I \;:\; X_i \neq \emptyset$$

- Let $X \neq \emptyset$ be a non-empty set, then a subset of the form $R \subseteq X \times X$ said to be a **relation** on X. And in this case it is customary to write xRy instead of $(x,y) \in R$. This notation will be used primarily for partial orders and equivalence relations (see below).

- The following concepts will be addressed in section 0.4 in greater detail. We just want to summarize the most important results for quick reference: Consider any non-empty set $X \neq \emptyset$ again. Then a relation $\sim$ on X is said to be an **equivalence relation** on X, iff it is *reflexive*, *symmetric* and *transitive*. Formally that is for any x, y and $z \in X$ we get

$$\begin{aligned} x = y &\quad\Longrightarrow\quad x \sim y \\ x \sim y &\quad\Longrightarrow\quad y \sim x \\ x \sim y,\; y \sim z &\quad\Longrightarrow\quad x \sim z \end{aligned}$$

And in this case we define the **equivalence class** $[x]$ of x to be the set of all $y \in X$ being equivalent to x, that is $[x] := \{ y \in X \mid x \sim y \}$. And the set of all equivalence classes is denoted by $X/\sim := \{ [x] \mid x \in X \}$. Example: If $f : X \to Y$ is any function then we obtain an equivalence relation $\sim$ on X by letting $x \sim y \iff f(x) = f(y)$. Then the equivalence class of $x \in X$ is just the fiber $[x] = f^{-1}(f(x))$.

- Consider a non-empty set $X \neq \emptyset$ once more. Then a family of subsets $\mathcal{P} \subseteq \mathcal{P}(X)$ is said to be a **partition** of X, iff for any $P, Q \in \mathcal{P}$ we obtain the statements

$$\begin{aligned} X &= \bigcup \mathcal{P} \\ P &\neq \emptyset \\ P \neq Q &\implies P \cap Q = \emptyset \end{aligned}$$

 Example: If $\sim$ is an equivalence relation on X, then $X/\sim$ is a partition of X. Conversely if $\mathcal{P}$ is a partition of X, then we obtain an equivalence relation $\sim$ on X by letting $x \sim y \iff \exists P \in \mathcal{P} :$ $x \in P$ and $y \in P$. Hence there is a one-to-one correspondence between the equivalence relations on X and the partitions of X given by $\sim \mapsto X/\sim$.

- Consider any non-empty set $I \neq \emptyset$, then a relation $\leq$ on I is said to be a **partial order** on I, iff it is *reflexive*, *transitive* and *anti-symmetric*. Formally that is for any i, j and $k \in I$ we get

$$\begin{aligned} i = j &\implies i \leq j \\ i \leq j,\ j \leq k &\implies i \leq k \\ i \leq j,\ j \leq i &\implies i = j \end{aligned}$$

 And $\leq$ is said to be a **total** or **linear order** iff for any i, $j \in I$ we also get $i \leq j$ or $j \leq i$ (that is any two elements contained in I can be compared). Example: For any set X the inclusion relation $\subseteq$ is a partial (but not linear) order on $\mathcal{P}(X)$. If now $\leq$ is a linear order on I, then we define the *minimum* and *maximum* of i, $j \in I$ to be

$$i \wedge j := \begin{cases} i \text{ if } i \leq j \\ j \text{ if } j \leq i \end{cases} \qquad i \vee j := \begin{cases} j \text{ if } i \leq j \\ i \text{ if } j \leq i \end{cases}$$

- Now consider a partial order $\leq$ on the set X and a subset $A \subseteq X$. Then we define the set A_* of **minimal** respectively the set A^* of **maximal** elements of A to be the following

$$\begin{aligned} A_* &:= \{ a_* \in A \mid \forall\, a \in A : a \leq a_* \implies a = a_* \} \\ A^* &:= \{ a^* \in A \mid \forall\, a \in A : a^* \leq a \implies a = a^* \} \end{aligned}$$

 And an element $a_* \in A_*$ is said to be a *minimal* element of A. Likewise $a^* \in A^*$ is said to be a *maximal* element of A. Note that in general it may happen that A has several minimal (or maximal) elements or even none at all (e.g. $\mathbb{N}_* = \{0\}$ and $\mathbb{N}^* = \emptyset$). For a linear order minimal (and maximal) elements are unique however.

- Finally $\leq$ is said to be a **well-ordering** on the set X, iff $\leq$ is a linear order on X such that any non-empty subset $A \subseteq X$ has a (already unique) minimal element. Formally that is

$$\forall \emptyset \neq A \subseteq X \ \exists a_* \in A \quad \text{such that} \quad \forall a \in A : a_* \leq a$$

- Let $X \neq \emptyset$ be a non-empty set, then the **cardinality** of X is defined to be the *class* of all sets that correspond bijectively to X. Formally that is

$$|X| \ := \ \{ Y \mid \exists \omega : X \to Y \text{ bijective} \}$$

Note that most textbooks on set theory define the cardinality to be a certain representative of our $|X|$ here. However the exact definition is of no importance to us, what matters is comparing cardinalities: We define the following relation $\leq$ between cardinals:

$$\begin{aligned} |X| \ \leq \ |Y| \quad &:\Longleftrightarrow \quad \exists \iota : X \to Y \text{ injective} \\ &\Longleftrightarrow \quad \exists \pi : Y \to X \text{ surjective} \\ |X| \ = \ |Y| \quad &:\Longleftrightarrow \quad \exists \omega : X \to Y \text{ bijective} \\ &\Longleftrightarrow \quad |X| \leq |Y| \ \text{ and } \ |Y| \leq |X| \end{aligned}$$

Note that the first equivalence can be proved (as a standard exercise) using equivalence relations and a choice function (axiom of choice). The second equivalence is a rather non-trivial statement called the equivalence theorem of Bernstein (0.32). However these equivalences grant that $\leq$ has the properties of a partial order, i.e. reflexivity, transitivity and anti-symmetry. In fact $\leq$ even acts as a total order, that is we either have $|X| \leq |Y|$ or $|X| \leq |X|$ or both.

- Suppose $x_1, x_2, \ldots, x_n$ are pairwise distinct elements. Then the set $X := \{ x_1, \ldots, x_n \}$ clearly has n elements. Using cardialities this would be expressed, as

$$| \{ x_1, \ldots, x_n \} | \ = \ |1 \ldots n|$$

In this case $1 \ldots n \longleftrightarrow X : i \mapsto x_i$ could be used as a bijection. Yet we also introduce less cumbersome notation - if $x_1, x_2, \ldots, x_n$ are pairwise distinct (that is $x_i = x_j \implies i = j$) we let

$$\# \{ x_1, \ldots, x_n \} \ := \ n$$

In particular $\#\emptyset = 0$. Hence for any finite set X we have defined the **number of elements** $\#X$. A set that is not finite is said to be infinite (see below). And in this case (if we don't care just how infinite X is, countable, uncountable or whatever) we write

$$\#X \ := \ \infty$$

- Thereby a set X is said to be **finite** iff there is some $n \in \mathbb{N}$ such that $X \longleftrightarrow (1 \ldots n)$, that is iff $\#X = n \in \mathbb{N}$. And we usually denote the set of all finite subsets of X by

$$\Omega(X) \ := \ \{ A \subseteq X \mid \#A < \infty \}$$

Likewise X is said to be **infinite**, iff $\mathbb{N}$ can be embedded into X, formally $\mathbb{N} \hookrightarrow X$ or in other words $|\mathbb{N}| \leq |X|$. Note that thereby we obtain a rather astounding equivalence of the statements

(a) X is infinite

(b) $|X| = |X \times X|$

(c) $|X| = |\Omega(X)|$

- If X and Y are finite, disjoint sets, then clearly $\#(X \cup Y) = (\#X) + (\#Y)$. Likewise for any finite sets X and Y we have $\#(X \times Y) = (\#X) \cdot (\#Y)$, $\#\mathcal{P}(X) = 2^{\#X}$ and $\#\mathcal{F}(X,Y) = (\#Y)^{\#X}$. We will use these properties to extend the ordinary arithmetic of natural numbers to the arithmetic of cardinal numbers, by defining

$$\begin{aligned} |X| + |Y| &:= |X \sqcup Y| \\ |X| \cdot |Y| &:= |X \times Y| \\ 2^{|X|} &:= |\mathcal{P}(X)| \\ |Y|^{|X|} &:= |\mathcal{F}(X,Y)| \end{aligned}$$

 for arbitrary sets X and Y. Note that $\sqcup$ refers to the *disjoint union* of X any Y, that is $X \sqcup Y := (\{1\} \times X) \cup (\{2\} \times Y)$. This is not necessary, if X and Y are disjoint to begin with, in this case we could have taken $X \cup Y$ right away. However in general we have to provide a way of separating X and Y and this nicely performed by $X \sqcup Y$. We will discuss cardinals in detail in section 0.5. It is a non-surprising but also non-trivial fact, that the power set of X is truly larger than X

$$|X| \;<\; |\mathcal{P}(X)|$$

- ($\diamondsuit$) We will introduce and use several different notions of substructures and isomorphy. In order to avoid eventual misconceptions, we emphasize the kinds of structures regarded by applying subscripts to the symbols $\leq$ and $\trianglelefteq$ of substructures and $\cong$ of isomorphy. E.g. we will write $R \leq_r S$ to indicate, that R is a sub-ring of S, $\mathfrak{a} \trianglelefteq_i R$ to indicate that $\mathfrak{a}$ is an ideal of R and $R \cong_r S$ to indicate that R and S are isomorphic as rings. Note that the latter is different from $R \cong_m S$ (R and S are isomorphic as modules). And this can well make sense, if $R \leq_r S$ is a sub-ring, then S can be regarded as an R-module, as well. We will use the same subscripts for generated algebraic substructures, i.e. $\langle \bullet \rangle_r$ for rings, $\langle \bullet \rangle_i$ for ideals and $\langle \bullet \rangle_m$ for modules. We are well aware that other authors do not introduce a formalism to keep track of the substructures and kind homomorphisms used, but we are convinced, that the exposition is far easier to understand, by doing so.

Notation

A, B, C	matrices, algebras and monoids
D, E, F	fields
G, H	groups and monoids
I, J, K	index sets
L, M, N	modules
P, Q	subsets and substructures
R, S, T	rings (all kinds of)
U, V, W	vector-spaces, multiplicatively closed sets
X, Y, Z	arbitrary sets
a, b, c	elements of rings
d, e	degree of polynomials, dimension
e	neutral element of a (group or) monoid
f, g, h	functions, polynomials and elements of algebras
i, j, k, l	integers and indexes
m, n	natural numbers
p, q	residue classes
r, s	further elements of rings
s, t, x	polynomial variables
u, v, w	elements of vector-spaces
x, y, z	elements of groups and modules
α, β, γ	multi-indexes
ι, κ	(canonical) monomorphisms
λ, μ	eigenvalues
μ, ν	valuation or Euclidean function
ϱ, σ	(canonical) epimorphisms
ϱ, σ, τ	permutations
φ, ψ	homomorphisms
Φ, Ψ	isomorphisms
Ω	(fixed) finite set
$\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$	ideals
$\mathfrak{u}$, $\mathfrak{v}$, $\mathfrak{w}$	other ideals
$\mathfrak{p}$, $\mathfrak{q}$	prime ideals
$\mathfrak{r}$, $\mathfrak{t}$	other prime ideals
$\mathfrak{m}$, $\mathfrak{n}$	maximal ideals
$\mathfrak{f}$, $\mathfrak{g}$, $\mathfrak{h}$	fraction ideals
$\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$	(ordered) bases or families of sets
$\mathcal{M}$, $\mathcal{N}$	more (ordered) bases
$\mathcal{E}$, $\mathcal{F}$	(canonical = Euclidean) bases

Part I

The Truth

0.4 A Primer on Sets

In this book we assume that the reader already is familiar with naive set theory, nevertheless we will present the most frequently used notions here. If you had troubles understanding the concepts in the previous section this will surely help, but we will not cover set theory in any depth.
It all began with Cantor's notion of a **set**: *A "set" is a collection M into a whole of definite, distinct objects m of our perception or thought.* True to this concept Cantor wrote $x \in M$ if the object x belongs to the set M (he said is an *element* of M) and $x \notin M$ if not. For example "Tuesday" is an element of the set of days in a week. Or the reader is an element of the set of all beings that are able to read English. Sets can even be infinite: A line is the set of all points that lie on it.

According to this definition, a set is completely determined by the elements it contains. That is the sets A and B are *equal*, iff they contain precisely the same elements. More explicitly this is the case iff for any object x (of our perception or thought) we have the equivalence

$$A = B \quad :\Longleftrightarrow \quad \big(x \in A \iff x \in B\big)$$

A related notion is that of a *subset* $A \subseteq B$: Intuitively speaking, that is A is contained in B (or may even be equal, but no larger than B). More formally this can be put as: We have $A \subseteq B$ if any element x of A already is contained in B, as well

$$A \subseteq B \quad :\Longleftrightarrow \quad \big(x \in A \implies x \in B\big)$$

From these definitions it is immediately clear (as $x \in A \implies x \in B$ and $x \in B \implies x \in A$ can be combined to $x \in A \iff x \in B$), that two sets A and B are equal iff they are mutually contained in each other. That is we have

$$A = B \iff \big(A \subseteq B \text{ and } B \subseteq A\big)$$

We will often use this fact to prove $A = B$ by showing both inclusions $A \subseteq B$ and $B \subseteq A$ separately. Cantor's notion also enables us to construct new sets from existing ones: E.g. the *intersection* $A \cap B$ is the set that contains the elements x that are both in A and in B. Likewise the *union* $A \cup B$ gathers all the objects x that come from at least one of these sets. And the *difference* $A \setminus B$ contains the elements $x \in A$, yet we scratch all objects x that also belong to B. Formally

$$\begin{aligned} A \cap B &:= \{\, x \mid x \in A \text{ and } x \in B \,\} \\ A \cup B &:= \{\, x \mid x \in A \text{ or } x \in B \,\} \\ A \setminus B &:= \{\, x \mid x \in A \text{ and } x \notin B \,\} \end{aligned}$$

Though this may not be entirely satisfactory from a formal point of view (mainly because the notion of an object x remains rather vague), this concept sustained mathematics for centuries. In the next section we will even refine this concept by presenting a list of *axioms* (that is statements, that we agree upon as being true, without question) that completely describe what we may safely do with sets.

This list of axioms will be (ZFC) [an abbreviation for Zermelo, Fraenkel plus the axiom of choice] that modern mathematics almost always uses. This also is the way formal set theory took: Hereby it is not explained what a set (object x) is. It just picks up a formal language containing the relation symbol $\in$ and deduces all the other theorems from the list (ZFC). It is thereby completely defined, what we may *do* with sets, but not what a set *is*. In this context a set is just a variable symbol x of the formal language speaking of sets. If you are inclined to learn how formal logic works, we recommend Many-Sorted Logic. Later in this book (when we come to category theory) we will also use classes. Naively speaking a **class** is just an arbitrary large collection of sets. Thereby it may well happen, that a certain class is a set again (if it contains not too many sets), but we have to separate these notions in order to avoid the contradictions, a devious mind may come up with. Again we will present a list (NBG) of axioms (which abbreviates Neumann, Bernays, Gödel) that describe how to deal with classes.
From a formal point of view we have a two-sorted language - one sort for sets and the other sort for classes. Then all the other theorems are deduced from (ZFC) appended by (NBG). So again formal mathematics does not answer what a class *is*, but evades the necessity to do so. Note that we will not say a word about naive or formal logic, but take this for granted. Our main focus are relations: Partial orders, equivalence relations and functions. But beforehand let us give a few examples of the workings of sets, that we will require later on, anyway:

(0.1) Example:

(i) If both $A, B \subseteq X$ are subsets of some larger set X, then the difference $A \setminus B$ is the intersection of A with the *complement* $X \setminus B$, formally put:

$$A \setminus B \;=\; A \cap \big(X \setminus B\big)$$

Prob by definition $X \setminus B = \{\, x \in X \mid x \notin B \,\}$. And as also $A \subseteq X$ we have $A = \{\, x \in X \mid x \in A \,\}$. Therefore $A \cap (X \setminus B) = \{\, x \in X \mid x \in A \text{ and } x \notin B \,\}$ and this is $A \setminus B$, again.

(ii) The *empty set* $\emptyset$ is the one ond only set, that does not contain any element at all. That is $x \in \emptyset$ is always false. Now for any sets A and B we have the equivalence of

$$A \subseteq B \iff \big(A \setminus B = \emptyset\big)$$

Prob to say $A \subseteq B$ is false, means that there is some $a \in A$ with $a \notin B$. In other words this is $a \in A \setminus B$ and hence $A \setminus B \neq \emptyset$. Hence (the negations of) these statements are equivalent.

(iii) Consider finitely many sets $B_1, \ldots, B_n$ and let $A := B_1 \cap B_2 \cap \cdots \cap B_n$ be the intersection of all of them. Then the following two statements are equivalent:

(a) $A = B_2 \cap \cdots \cap B_n$

(b) $B_2 \cap \cdots \cap B_n \subseteq B_1$

Prob (a) $\implies$ (b) is easy: If $b \in B_2 \cap \cdots \cap B_n = A$ we find $b \in A = B_1 \cap \cdots \cap B_n \subseteq B_1$ by construction of A. Conversely for (b) $\implies$ (a) we directly see $A = B_1 \cap \cdots \cap B_n \subseteq B_2 \cap \cdots \cap B_n$. For $B_2 \cap \cdots \cap B_n \subseteq A$ consider any $a \in B_2 \cap \cdots \cap B_n \subseteq B$. Then $a \in B_1 \cap (B_2 \cap \cdots \cap B_2) = A$.

(0.2) Proposition: (viz. 682)
Let I and J be any non-empty index sets and for $i \in I$ respectively for any $j \in J$ let A_i and B_j be arbitrary sets. Also consider some sets A and B. Then we get the following identities

$$\left(\bigcup_{i\in I} A_i\right) \cap B \;=\; \bigcup_{i\in I} (A_i \cap B)$$

$$\left(\bigcap_{i\in I} A_i\right) \cup B \;=\; \bigcap_{i\in I} (A_i \cup B)$$

$$\left(\bigcup_{i\in I} A_i\right) \cap \left(\bigcup_{j\in J} B_j\right) \;=\; \bigcup_{(i,j)\in I\times J} (A_i \cap B_j)$$

$$\left(\bigcap_{i\in I} A_i\right) \cup \left(\bigcap_{j\in J} B_j\right) \;=\; \bigcap_{(i,j)\in I\times J} (A_i \cup B_j)$$

And if for any $i \in I$ we have $A_i \subseteq X$, where X is any other set, then we also find the following identities for the *complements* $X \setminus A$

$$X \setminus \bigcup_{i\in I} A_i \;=\; \bigcap_{i\in I} (X \setminus A_i)$$

$$X \setminus \bigcap_{i\in I} A_i \;=\; \bigcup_{i\in I} (X \setminus A_i)$$

Relations and Functions

(0.3) Definition:
If X and Y are any sets, then a **relation** R between these sets is just a subset of the cartesian product of X and Y, formally

$$R \;\subseteq\; X \times Y$$

We say that the elements $x \in X$ and $y \in Y$ are **related** under R, if the ordered pair $(x,y) \in X \times Y$ is contained in R. In this case we write xRy, in formal terms

$$x\,R\,y \;:\Longleftrightarrow\; (x,y) \in R$$

(0.4) Remark: (viz. 681)
The cartesian product $X \times Y$ is thought to be the set of all pairs (x,y) where $x \in X$ and $y \in Y$. Formally we could define (x,y) to be

$$(x,y) \;:=\; \{\, x, \{\, x, y \,\}\,\}$$

Using this construction it can be proved (distinguishing 8 cases and using the axiom of foundation) that for any u, $x \in X$ and any v, $y \in Y$ we have the desired property of ordered pairs

$$(u,v) \;=\; (x,y) \;\Longleftrightarrow\; u = x \text{ and } v = y$$

(0.5) Definition:
If X and Y are any sets again, then a **partial function** f is a relation between X and Y that is *right unique* in the following sense: For any $x \in X$ and any $y_1, y_2 \in Y$ we have the implication

$$x f y_1 \text{ and } x f y_2 \implies y_1 = y_2$$

In this case we will write $f : X \rightarrowtail Y$ and given $x \in X$ and $y \in Y$ we will often rewrite the relation f in the following form

$$f : x \mapsto y \quad :\Longleftrightarrow \quad x f y$$

We will denote by $f(x)$ the unique element $y \in Y$ such that xfy (if this exists). And we define the **domain** of f to be the set of all $x \in X$ that are assigned some value $y \in Y$

$$\operatorname{dom}(f) \;:=\; \{\, x \in X \mid \exists\, y \in Y : x f y \,\}$$

And a partial function is said to be a **function**, iff it is *left total* in the following sense: For any $x \in X$ there is some $y \in Y$ such that xfy. Thus a function f is a relation that satisfies

$$\forall\, x \in X \;\; \exists !\, y \in Y \;\; : \;\; x f y$$

In other words again that is $\operatorname{dom}(f) = X$. Thereby a partial function $f : X \rightarrowtail Y$ always is a function $f : \operatorname{dom}(f) \to Y$. The set of all functions from X to Y will be denoted by

$$\mathcal{F}(X,Y) \;=\; Y^X \;:=\; \{\, f \subseteq X \times Y \mid f \text{ is a function} \,\}$$

If now $A \subseteq X$ and $B \subseteq Y$ are any subsets of X and Y respectively then we define the **image** of A and **preimage** of B under f to be the following sets

$$\begin{aligned} f(A) \;&:=\; \{\, f(x) \mid x \in A \,\} \;\subseteq\; Y \\ f^{-1}(B) \;&:=\; \{\, x \in X \mid f(x) \in B \,\} \;\subseteq\; X \end{aligned}$$

(0.6) Remark:
Intuitively speaking a function is a black box, that assigns every $x \in X$ some value $y = f(x) \in Y$. To use a relation as the general framework just is a neat trick to pull functions back into the concept of sets. In fact this notion is so predominant that one oven introduces a symbol to get f back from f: The **graph** of f is defined to be

$$\Gamma(f) \;:=\; \{\, (x,y) \in X \times Y \mid y = f(x) \,\} \;=\; f$$

We will often encounter the following situation: Given sets X, Y and some $x \in X$ we define some $f(x)$. Then we need to prove that $f : X \to Y$ with $f : x \mapsto f(x)$ is a **well-defined** function $f : X \to Y$. This is to say we have to check the following properties: (1) First of all for any $x \in X$ the element $f(x)$ needs to be an element of $f(x) \in Y$. And (2) if x_1 and $x_2 \in X$ such that $x_1 = x_2$ then we need $f(x_1) = f(x_2)$. This is the right uniqueness of f. That is we have a partial function $f :\rightarrowtail Y$. If we made no restriction as to what $x \in X$ we take, f already is a function from X to Y.

(0.7) Proposition: (viz. 683)
Let X and Y be arbitrary sets, $A \subseteq X$ and $B \subseteq Y$ be subsets and consider a function $f : X \to Y$. Then we get all of the following statements

$$\begin{array}{rcl} A & \subseteq & f^{-1}\big(f(A)\big) \\ f(X) \cap B & = & f\big(f^{-1}(B)\big) \\ X \setminus f^{-1}(B) & = & f^{-1}\big(Y \setminus B\big) \\ f(A) \subseteq B & \iff & A \subseteq f^{-1}(B) \end{array}$$

In particular $f\big(f^{-1}(B)\big) \subseteq B$. If now $\mathcal{A} = \{ A_i \mid i \in I \}$ is an entire collection of subsets $A_i \subseteq X$ and $\mathcal{B} = \{ B_j \mid j \in j \}$ be a collection of subsets of Y, then we further get

$$\begin{array}{rcl} f^{-1}\left(\bigcup\limits_{j\in J} B_j\right) & = & \bigcup\limits_{j\in J} f^{-1}(B_j) \\ f^{-1}\left(\bigcap\limits_{j\in J} B_j\right) & = & \bigcap\limits_{j\in J} f^{-1}(B_j) \\ f\left(\bigcup\limits_{i\in I} A_i\right) & = & \bigcup\limits_{i\in I} f(A_i) \\ f\left(\bigcap\limits_{i\in I} A_i\right) & \subseteq & \bigcap\limits_{i\in I} f(A_i) \end{array}$$

($\diamondsuit$) Note that in the cases where we have an inclusion $\subseteq$ only, then equality need not be true in general. However if f is *injective* (see below), then in both cases we have the equality of sets

$$\begin{array}{rcl} A & = & f^{-1}\big(f(A)\big) \\ f\left(\bigcap\limits_{i\in I} A_i\right) & = & \bigcap\limits_{i\in I} f(A_i) \end{array}$$

(0.8) Definition:
Let now X, Y and Z be sets, $A \subseteq X$ be a subset and consider the functions $f : X \to Y$ and $g : Y \to Z$. First of all we define the **restriction** of f to A to be the following function

$$f\big|_A \;:=\; \{ (x,y) \mid x \in A,\, y = f(x) \}$$

In particular the restriction $f|_A$ is a function of the form $A \to Y$ given by $f|_A : x \mapsto f(x)$. And we also define the **composition** gf of g **after** f to be the following function

$$gf \;:=\; \{ (x,z) \in X \times Z \mid \exists\, y \in Y \,:\, y = f(x) \text{ and } z = g(y) \}$$

In particular gf is a function of the form $X \to Z$ that takes $x \in X$ to $y = f(x) \in Y$ and further on to $z = g(y) \in Z$. That is we can write

$$gf \;:\; X \to Z \;:\; x \;\mapsto\; g\big(f(x)\big)$$

(0.9) Remark:
Note that thereby the composition of maps is associative: That is for any chain of functions $f : U \to X$, $g : X \to Y$ and $h := Y \to Z$ we get $(hg)f = h(gf)$ as for any $u \in U$ we have

$$\big((hg)f\big)(u) \;=\; hg\big(f(u)\big) \;=\; h\big(g\big(f(u)\big)\big) \;=\; h\big(gf(u)\big) \;=\; \big(h(gf)\big)(u)$$

(0.10) Definition: (viz. 685)
Let X and Y be arbitrary sets, $f : X \to Y$ be a function from X to Y. Then f is said to be **injective**, iff it satisfies any one of the following four equivalent properties. And in this case we write $f : X \hookrightarrow Y$.

(a) The function f admits a *left-inverse*, that is there is some function $g : Y \to X$ such that the composition satisfies

$$gf \;=\; \mathbb{1}_X$$

(b) Separate points of X will be assigned separate points in Y: That is for any u, $x \in X$ we obtain the following implication

$$f(u) \;=\; f(x) \quad\Longrightarrow\quad u \;=\; x$$

(c) For any subset $A \subseteq X$ the preimage of the image of A is just A again

$$f^{-1}\big(f(A)\big) \;=\; A$$

(d) Every *fiber* of f contains at most one element: That is for any $y \in Y$

$$\#f^{-1}\big(\{y\}\big) \;\leq\; 1$$

And $f : X \to Y$ is said to be **surjective**, iff it satisfies any one of the following four equivalent properties. Likewise we introduce the notation $f : X \twoheadrightarrow Y$ to abbreviate (emphasize) this case.

(a) The function f admits a *right-inverse* that is there is some function $g : Y \to X$ such that the composition satisfies

$$fg \;=\; \mathbb{1}_Y$$

(b) The function f reaches the entire set Y, that is the *image* of f is Y

$$f(X) \;=\; Y$$

(c) For any subset $B \subseteq Y$ the image of the preimage of B is just B again

$$f\big(f^{-1}(B)\big) \;=\; B$$

(d) Every *fiber* of f contains at least one element: That is for any $y \in Y$

$$\#f^{-1}\big(\{y\}\big) \;\geq\; 1$$

Finally $f : X \to Y$ is said to be **bijective**, iff it satisfies any one of the following four equivalent properties. And in this case we write $f : X \longleftrightarrow Y$.

(a) The function f is a one-to-one correspondence between the elements of X and the elements of Y, that is for any $y \in Y$ there is a uniquely determined $x \in X$ such that $y = f(x)$. Formally

$$\forall\, y \in Y \;\; \exists !\, x \in X \;\; : \;\; y \;=\; f(x)$$

(b) The function f has a uniquely defined **inverse function** $f^{-1} : Y \to X$ whose compositions satisfy

$$f^{-1}f \;=\; \mathbb{1}_X \quad \text{and} \quad ff^{-1} \;=\; \mathbb{1}_Y$$

(c) The function f admits both, a *left-inverse* function $\ell : Y \to R$ and a *right-inverse* function $r : Y \to X$ that is ℓ and r satisfy the properties

$$\ell f \;=\; \mathbb{1}_X \quad \text{and} \quad fr \;=\; \mathbb{1}_Y$$

(d) The function f is both: injective and bijective.

(0.11) Remark:
For the time being f^{-1} is just a peculiar name for the inverse function of f. It has the advantage of designating the function f it came from however. This is useful as [due to the symmetry of property (b)] f is the inverse function of f^{-1}. Later we will denote the inverse element of some element $x \in G$ of a group G by x^{-1}. This is consistent, as f^{-1} is precisely the inverse element of f in the group of bijective functions from X to Y.

Equivalence Relations

(0.12) Definition:
Let X be a set and consider an arbitrary collection $\mathcal{A} = \{\, A_i \mid i \in I \,\}$ of subsets $A_i \subseteq X$. Then we say that $\mathcal{A}$ is a **partition** of X iff the $A_i \in \mathcal{A}$ are non-empty, pairwise disjoint and X is the grand union of $\mathcal{A}$. That is we get the following properties

$$\begin{array}{lrcl}
(1) & \forall\, A_i \in \mathcal{A} & : & A_i \neq \emptyset \\
(2) & \forall\, A_i, A_j \in \mathcal{A} & : & A_i \cap A_j \neq \emptyset \implies A_i = A_j \\
(3) & X & = & \bigcup_{i \in I} A_i
\end{array}$$

And a relation of the form $\sim \;\subseteq\; X \times X$ is said to be an **equivalence relation** iff it is reflexive, symmetric and transitive. That is for any x, y and $z \in X$ we find the following properties for $\sim$

$$\begin{array}{lrcl}
(1) & & & x \sim x \\
(2) & x \sim y & \implies & y \sim x \\
(3) & x \sim y,\; y \sim z & \implies & x \sim z
\end{array}$$

If $\sim$ is an equivalence relation on X and $x \in X$ is any element, then we define the **equivalence class** of x to be the following subset of X

$$[x] \;:=\; \{\, u \in X \mid u \sim x \,\}$$

Note that (by construction of the equivalence classes $[x]$) for any $x, y \in X$ the following statements are equivalent (a) $x \sim y$, (b) $[x] = [y]$ and (c) $x \in [y]$. And the collection of all equivalence classes of $\sim$ will be denoted as (note that the definition of this set will most certainly contain redundancies $[u] = [x]$)

$$X\big/_{\sim} \;:=\; \{\, [x] \mid x \in X \,\}$$

(0.13) Lemma: (viz. 686)
If $X \neq \emptyset$ is a non-empty set then there is a one-to-one correspondence between the partitions of X and the equivalence relations on X. That is if we denote the sets

$$\begin{aligned} \mathrm{part}(X) &:= \{\, \mathcal{A} \subseteq \mathcal{P}(X) \mid \mathcal{A} \text{ is a partition} \,\} \\ \mathrm{equi}(X) &:= \{\, \sim \subseteq X \times X \mid \sim \text{ is an equivalence relation} \,\} \end{aligned}$$

then the following map from the set of equivalence relations on X to the set of partitions of X is well-defined and bijective

$$\mathrm{equi}(X) \;\longleftrightarrow\; \mathrm{part}(X) \;:\; \sim \;\mapsto\; X\big/_{\sim}$$

Thereby the inverse function of this map is given by the following construction: If $\mathcal{A}$ is a partition of X and $u, x \in X$ we define the relation

$$u \sim_{\mathcal{A}} x \quad :\Longleftrightarrow \quad \exists\, A \in \mathcal{A} \;:\; \{\, u, x \,\} \;\subseteq\; A$$

(0.14) Remark:
Equivalence relations are *the* primary tool to isolate a problem or property. And they frequently call for a check of *well-definedness* of a function: Consider any two sets X and Y, a function $f : X \to Y$ and an equivalence relation $\sim$ on X. Then we say that f *factors* through $\sim$, iff for any $x, y \in X$ we get

$$x \sim y \quad \Longrightarrow \quad f(x) \,=\, f(y)$$

Let us denote the quotient set $A := X/\sim$, then this property enables us to define a function $\overline{f} : A \to Y$ by letting $\overline{f}(a) := f(x)$ where $a = [x]$ for some $x \in X$. Note that the factors-property is exactly what we need to guarantee, that $f(x)$ does not depend on the choice of the specific $x \in a \in A$. Also note that - by going to equivalence classes - the factors-property of f is just the same, as the well-definedness-property of $\overline{f}$. The latter reads as: For any $a, b \in A$ we have

$$a \,=\, b \quad \Longrightarrow \quad \overline{f}(a) \,=\, \overline{f}(b)$$

This is the standard case, when we say that we need to check the well-definedness of a function $\overline{f}$ defined on equivalence classes. And while this actually is the second implication for a and b, this is just an equivalent formulation of the first implication for x and y. And it is this first formulation, that we will verify to get the well-definedess of $\overline{f}$.

(0.15) Example:
If X and Y are sets, $f : X \to Y$ is any function, then we obtain an equivalence relation $\sim_f$ of X by defining (for any $u, y \in X$)

$$u \sim_f x \quad :\Longleftrightarrow \quad f(u) \;=\; f(x)$$

It is clear that this relation is reflexive, symmetric and transitive (as the equality relation $=$ satisfies all these properties). And for any $x \in X$ the equivalence of x is precisely the fibre of $f(x) \in Y$, that is

$$[x] \;=\; f^{-1}\big(\,\{\,f(x)\,\}\,\big) \;\subseteq\; X$$

In this case it is clear - by construction - that f factors through $\sim_f$ and thereby we obtain a well-defined, even injective, function $\overline{f}$ on the set of quotients

$$\overline{f} \;:\; X\Big/_{\sim} \;\hookrightarrow\; Y \;:\; [x] \mapsto f(x)$$

(0.16) Remark:
If $\sim$ is an equivalence relation on the set X, then the set $X/\sim$ of equivalence classes is a partition of X. In particular any $A \in X/\sim$ is non-empty and hence the axiom of choice guarantees, that there is a set $R \subseteq X$ such that we have a one-to-one correspondence

$$R \;\longleftrightarrow\; X\Big/_{\sim} \;:\; x \mapsto [x]$$

Such a set R is called a **system of representatives** of the relation $\sim$. And with such a system we have (without redundancies this time)

$$X\Big/_{\sim} \;=\; \{\,[x] \mid x \in R\,\}$$

Partial and Total Orders

(0.17) Definition:
Let X be a set and $\leq \subseteq X \times X$ be a relation on X. Then we say that $\leq$ is a **partial order** on X, iff it is reflexive, transitive and antisymmetric. That is for any x, y and $z \in X$ we find the properties

$$\begin{array}{lll} (1) & & x \leq x \\ (2) & x \leq y,\; y \leq z & \Longrightarrow \quad x \leq z \\ (3) & x \leq y,\; y \leq x & \Longrightarrow \quad x = y \end{array}$$

In this case, if $A \subseteq X$ is any subset, we define the abbreviations $x \leq A \;:\Longleftrightarrow\; \forall\, a \in A : x \leq A$ and $A \leq x \;:\Longleftrightarrow\; \forall\, a \in A : a \leq x$. And a partial order $\leq$ is said to be a **total order** or alternatively **linear order**, iff it satisfies the following fourth property

$$(4)\;\; \forall\, x, y \in X \;\;:\;\; x \leq y \;\text{ or }\; y \leq x$$

If $\leq$ is a partial [resp. total] order, then the pair $(X, \leq)$ is called a **partially ordered** [resp. **totally ordered**] **set**. In the literature this is sometimes abbreviated as *poset* or *toset* respectively. In any case a subset $N \subseteq X$ is said to be a **net** in $(X, \leq)$ iff every two elements of N have a common greater element, that is

$$\forall\, x, y \in N \;\; \exists z \in N \;\; : \;\; x \leq z \;\text{ and }\; y \leq z$$

And a subset $C \subseteq X$ said to be a **chain** in $(X, \leq)$ iff is a totally ordered set under the order $\leq$ inherited from X. That is iff for any two elements of C we can decide which one is the greater, formally

$$\forall\, x, y \in C \;\; : \;\; x \leq y \;\text{ or }\; y \leq x$$

Let us denote the set of all nets, resp. of all chains resp. of all finite chains in $(X, \leq)$ by $\mathcal{N}(X, \leq)$, $\mathcal{C}(X, \leq)$ and $\mathcal{C}_0(X, \leq)$, that is we denote the following collections of subsets of X

$$\begin{aligned} \mathcal{N}(X, \leq) &:= \{\, N \subseteq X \mid C \text{ net} \,\} \\ \mathcal{C}(X, \leq) &:= \{\, C \subseteq X \mid C \text{ chain} \,\} \\ \mathcal{C}_0(X, \leq) &:= \{\, C \subseteq X \mid C \text{ chain}, \#C < \infty \,\} \end{aligned}$$

Any chain already is a net [given $x, y \in C$ just let $z := \max\{ x, y \}$ then $x \leq z$ and $y \leq z$ are obvious], therefore these sets satisfy the inclusions

$$\mathcal{C}_0(X, \leq) \;\subseteq\; \mathcal{C}(X, \leq) \;\subseteq\; \mathcal{N}(X, \leq)$$

Finally if $A \subseteq X$ is any subset and $(X, \leq)$ is a partially ordered set again, then we define the following notions concerning elements of X

(i) An element $g \in X$ is called the **greatest element** of A iff $g \in A$ and for any $a \in A$ we have $a \leq g$. If it exists the greatest element of A is uniquely determined and will be denoted

$$\max(A) \;:=\; g$$

An element $\ell \in X$ is called the **least element** of A iff $\ell \in A$ and for any $a \in A$ we have $\ell \leq a$. If it exists the least element of A is uniquely determined and will be denoted

$$\min(A) \;:=\; \ell$$

Prob suppose both g and g' are greatest elements of A. As $g \in A$ and g' is a greatest element we have $g \leq g'$. Vice versa we have $g' \leq g$. So by anti-symmetry of $\leq$ we find $g = g'$. The same reasoning can be applied to the least elements of A.

(ii) An element $m \in X$ is called a **maximal element** of A iff $m \in A$ and for any $a \in A$ we have the implication $m \leq a \implies a = m$. The set of maximal elements of A will be denoted by

$$A^* \;:=\; \{\, m \in A \mid \forall\, a \in A : m \leq a \implies a = m \,\}$$

Likewise an element $m \in X$ is called a **minimal element** of A iff $m \in A$ and for any $a \in A$ we have the implication $a \leq m \implies a = m$. The set of minimal elements of A will be denoted by

$$A_* \;:=\; \{\, m \in A \mid \forall\, a \in A : a \leq m \implies a = m \,\}$$

(0.18) Remark:

(i) Let X be any set, recall the definition of the **power set** to be the set of all subsets of X, that is

$$\mathcal{P}(X) \;=\; \{\, A \mid A \subseteq X \,\}$$

A special case is the power set of the empty set, which is $\mathcal{P}(\emptyset) = \{\emptyset\}$. And e.g. for $X = \{1,2,3\}$ the power set is given to be

$$\mathcal{P}(X) \;=\; \{\emptyset,\, \{1\},\, \{2\},\, \{3\},\, \{1,2\},\, \{1,3\},\, \{2,3\},\, X\}$$

In general $\mathcal{P}(X)$ contains $2^{|X|}$ elements. Thereby $(\mathcal{P}(X), \subseteq)$ is a partially ordered set for any set X, however $\subseteq$ is not a total order. This can already be seen in the example here: The subsets $\{1,2\}$ and $\{1,3\}$ of X are not *comparable* under $\subseteq$, as we neither have $\{1,2\} \subseteq \{1,3\}$ nor $\{1,3\} \subseteq \{1,2\}$. Thus $\subseteq$ is not a total order on X.

(ii) If $(X, \leq)$ is a partially [resp. totally] ordered set and $A \subseteq X$ is a subset, then the restriction $(\leq \cap\, A \times A) \subseteq A \times A$ is a partial [resp. total] order on A. That is for any $a, b \in A$ we let $a \leq b$ be true, if and only $a \leq b$ when we regard a and b as elements of X. By abuse of notation we write $\leq$ for the restricted order as well, that is $(A, \leq)$ is a partially [resp. totally] ordered set again.

(iii) In particular any collection $\mathcal{A} \subseteq \mathcal{P}(X)$ of subsets of an arbitrary set X is partially ordered under inclusion $\subseteq$ again, that is

$$(\mathcal{A}, \subseteq) \text{ is a partially ordered set}$$

(iv) Let us continue with the example $X = \{1,2,3\}$ and regard the collection $\mathcal{A} := \mathcal{P}(X) \setminus \{\emptyset, X\}$ of non-trivial subsets of X. Explicitly this $\mathcal{A}$ is given to be

$$\mathcal{A} \;=\; \{\{1\},\, \{2\},\, \{3\},\, \{1,2\},\, \{1,3\},\, \{2,3\}\}$$

Then $\mathcal{A}$ has 3 maximal elements, namely $\{1,2\}$, $\{1,3\}$ and $\{2,3\}$. That is the set of maximal elements of $\mathcal{A}$ is given to be the following subset of $\mathcal{A}$

$$\mathcal{A}^* \;=\; \{\{1,2\}, \{1,3\}, \{2,3\}\}$$

(v) (■) Probably the most important example of all are the natural numbers $\mathbb{N}$. They admit an ordering $m \leq n \;:\Longleftrightarrow\; \exists\, k \in \mathbb{N} : m + k = n$ that even is a well-ordering. That is any non-empty subset $N \subseteq \mathbb{N}$ has a least element. The reader is asked to consult any textbook on "numbers" for a construction of $\mathbb{N}$ and a proof of this theorem.

(0.19) Proposition: (viz. 687)
If $(X, \leq)$ is a partially ordered set and $F \subseteq X$ is a non-empty, finite subset of X, then F contains at least one maximal and one minimal element

$$F^* \neq \emptyset \quad \text{and} \quad F_* \neq \emptyset$$

If $(X, \leq)$ is a totally ordered set and $F \subseteq X$ is a non-empty, finite subset of X, then F has both a greatest and a least element

$$\exists!\, g, \ell \in F \;:\; \max(F) = g \;\text{ and }\; \min(F) = \ell$$

(0.20) Proposition: (viz. 688)
If $(X, \leq)$ is a totally ordered set and $x_1, \ldots, x_n \in X$ are finitely may elements of X (where $2 \leq n \in \mathbb{N}$), then the minimum and maximum of $\{ x_1, \ldots, x_n \}$ can be evaluated sequentially. Formally this means

$$\min\{ \min\{ x_1, \ldots, x_{n-1} \}, x_n \} \;=\; \min\{ x_1, \ldots, x_n \} \;=\; \min\{ x_1, \min\{ x_2, \ldots, x_n \} \}$$

$$\max\{ \max\{ x_1, \ldots, x_{n-1} \}, x_n \} \;=\; \max\{ x_1, \ldots, x_n \} \;=\; \max\{ x_1, \min\{ x_2, \ldots, x_n \} \}$$

Nota if we denote the minimum of two elements $x, y \in X$ by $x \wedge y := \min\{ x, y \} \in X$ and likewise the maximum, by $x \vee y := \max\{ x, y \}$, then in particular we find the *associativity* of the operations $\wedge$ and $\vee$

$$(x \wedge y) \wedge z \;=\; x \wedge (y \wedge z) \quad \text{and} \quad (x \vee y) \vee z \;=\; x \vee (y \vee z)$$

(0.21) Proposition: (viz. 688)
If $(X, \leq)$ is a partially ordered set and for any $i \in I$ we consider a chain $C_i \in \mathcal{C}(X, \leq)$ (where $I \neq \emptyset$ is an arbitrary index set), then their intersection is a chain in X again

$$\bigcap_{i \in I} C_i \;\in\; \mathcal{C}(X, \leq)$$

Now suppose the C_i not only are chains, but that $\{ C_i \mid i \in I \}$ also is a net under inclusion [i.e. it is a net in the partially ordered set $(\mathcal{P}(X), \subseteq)$] then their union is a chain in X, as well

$$\bigcup_{i \in I} C_i \;\in\; \mathcal{C}(X, \leq)$$

0.5 Some Tools from Set Theory

After we have introduced the basic concepts of naive set theory (how to use sets, functions, equivalence relations an partial orders) let us dig a little deeper: Some concepts of algebra are general truisms on the level of sets, already, like chain conditions and Galois connections. In the algebraic setting these basic concepts will only be enriched by additional properties or equivalences.
On the other hand set theory provides some very powerful tools, that we really need. Primarily the lemma of Zorn, which provides the most often used construction, right after equivalence relations. And finally don't want to start without going into a little more detail when it comes to comparing cardinalities.
Let us start with an easy concept: Galois connections. The relation between sets of polynomials and their common roots will be a Galois connection. Likewise the transfer of ideals in ring-extensions and the relation between prime ideals over an ideal and their intersection. And lastly the relation between intermediate fields and their Galois group will be a Galois connection - this is where the name comes from. Most of these connections will be contra-variant, so the covariant case is of lesser interest to us. Also it just is the same thing without reversing the order - not a genuinely new concept. As is we have three good reasons to study Galois connections in general:

Galois Connections

If $(X,\leq)$ and $(Y,\leq)$ are partially ordered set then a function $f : X \to Y$ is said to be *monotonous*, iff $x \leq y$ implies $f(x) \leq f(y)$. In other words f is *order-preserving*. If conversely $x \leq y$ implies $f(x) \geq f(y)$, then f is said to be *antitonous* or *order-reversing*. The following situation (this might come as a surprise) is rather commonplace - we will encounter it several times:

(0.22) Definition: (viz. 688)
Let $(X,\leq)$ and $(Y,\leq)$ be two partially ordered sets and let $f : X \to Y$ and $g : Y \to X$ be two *order-reversing* functions, that is for any x, $x' \in X$ and any y, $y' \in Y$ we have the implications

$$\begin{aligned} x \leq x' &\implies f(x') \leq f(x) \\ y \leq y' &\implies g(y') \leq g(y) \end{aligned}$$

Then the following three statements are equivalent. And in this case we say that (f,g) is a **Galois connection** between $(X,\leq)$ and $(Y,\leq)$:

(a) $\forall\, x \in X, \forall\, y \in Y \;:\; x \leq g(y) \iff y \leq f(x)$

(b) $\forall\, x \in X, \forall\, y \in Y \;:\; x \leq gf(x)$ and $y \leq fg(y)$

(c) For any $x \in X$ the element $f(x) \in Y$ is the greatest element of Y, that satisfies $x \leq g(y)$ and likewise for g. That is (for any $x \in X$ and any $y \in Y$) we have

$$\begin{aligned} f(x) &= \max\{\, y \in Y \mid x \leq g(y) \,\} \\ g(y) &= \max\{\, x \in X \mid y \leq f(x) \,\} \end{aligned}$$

And in this case these maps satisfy $fgf = f$ and $gfg = g$. In other words the functions f and g give rise to a one-to-one correspondence between their respective image sets. The following map is bijective:

$$\begin{array}{rcl} g(Y) & \longleftrightarrow & f(X) \\ x & \mapsto & f(x) \\ g(y) & \hookleftarrow & y \end{array}$$

(0.23) Example:
The properties $fgf = f$ and $gfg = g$ alone do not suffice for a Galois connection however. As an example take $X := \{1,2,3\}$ and $Y := \{1,2\}$ under the natural order of $\mathbb{N}$. Then define f by $f(1) := 2$, $f(2) := 1$ and $f(3) := 1$. Likewise $g(1) := 2$ and $g(2) := 1$. Then straightforward to check that we get the one-to-one correspondence $\{1,2\} \longleftrightarrow \{1,2\}$ but $gf(3) = 2$ does not satisfy $3 \leq gf(3)$, that is (b) is not satisfied.

(0.24) Remark:
The above version of a Galois connection is *contra-variant*. There also is a *covariant* version, in which $f : X \to Y$ and $g : Y \to X$ are two *order-preserving* functions, that is for any x, $x' \in X$ and any y, $y' \in Y$ we have the implications

$$\begin{array}{rcl} x \leq x' & \Longrightarrow & f(x) \leq f(x') \\ y \leq y' & \Longrightarrow & g(y) \leq g(y') \end{array}$$

Then the following three statements are equivalent. And in this case we say that (f,g) is a **Galois connection** between $(X,\leq)$ and $(Y,\leq)$:

(a) $\forall\, x \in X, \forall\, y \in Y \;:\; f(x) \leq y \iff x \leq g(y)$

(b) $\forall\, x \in X, \forall\, y \in Y \;:\; x \leq gf(x)$ and $fg(y) \leq y$

(c) For any $x \in X$ the element $f(x) \in Y$ is the least element of Y, that satisfies $x \leq g(y)$ and $g(y)$ is the greatest element of X, that satisfies $f(x) \leq y$. That is (for any $x \in X$ and any $y \in Y$) we have

$$\begin{array}{rcl} f(x) & = & \min\{\, y \in Y \mid x \leq g(y) \,\} \\ g(y) & = & \max\{\, x \in X \mid f(x) \leq y \,\} \end{array}$$

And in this case these maps satisfy $fgf = f$ and $gfg = g$. In other words the functions f and g give rise to a one-to-one correspondence between their respective image sets, just as in the contra-variant case:

$$\begin{array}{rcl} g(Y) & \longleftrightarrow & f(X) \\ x & \mapsto & f(x) \\ g(y) & \hookleftarrow & y \end{array}$$

(0.25) Definition: (viz. 689)
Let $(X, \leq)$ be a partially ordered set, then we say that $(X, \leq)$ satisfies the **ascending chain condition** (which we will always abbreviate by **ACC**), iff it satisfies one of the following two equivalent properties

(a) Any non-empty $A \neq \emptyset$ subset $A \subseteq X$ of X has a maximal element. That is there is some $a^* \in A$ such that

$$\forall\, a \in A \;:\; a \leq a^* \implies a = a^*$$

(b) Any ascending chain within X stabilizes, that is for any $(x_k) \subseteq X$ (where $k \in \mathbb{N}$) such that $x_0 \leq x_1 \leq x_2 \leq \ldots$ we have

$$\exists\, s \in \mathbb{N}\ \forall\, i \in \mathbb{N} \;:\; x_{s+i} = x_s$$

In complete analogy we we say that $(X, \leq)$ satisfies the **descending chain condition** (which we will always abbreviate by **DCC**), iff it satisfies one of the following two equivalent properties

(a) Any non-empty $A \neq \emptyset$ subset $A \subseteq X$ of X has a minimal element. That is there is some $a_* \in A$ such that

$$\forall\, a \in A \;:\; a_* \leq a \implies a = a_*$$

(b) Any descending chain within X stabilizes, that is for any $(x_k) \subseteq X$ (where $k \in \mathbb{N}$) such that $x_0 \geq x_1 \geq x_2 \geq \ldots$ we have

$$\exists\, s \in \mathbb{N}\ \forall\, i \in \mathbb{N} \;:\; x_{s+i} = x_s$$

(0.26) Lemma: (viz. 690)
Let $(X, \leq)$ be a partially ordered set and recall that $\mathcal{C}(X, \leq)$ denotes the set of all chains, $\mathcal{C}_0(X, \leq)$ denotes the set of finite chains of $(X, \leq)$. Then the following three statements are equivalent

(a) $(X, \leq)$ satisfies both ACC and DCC

(b) $(\mathcal{C}_0(X, \leq), \subseteq)$ satisfies ACC

(c) Every chain in $(X, \leq)$ is finite, that is the have the equality of the sets

$$\mathcal{C}(X, \leq) \;=\; \mathcal{C}_0(X, \leq)$$

And in this case any chain in $(X, \leq)$ can be refined to a maximal finite chain, that is: If $C \subseteq X$ is a chain in $(X, \leq)$, then there is some $C^* \in \mathcal{C}_0(X, \leq)$ such that $C \subseteq C^*$ and

$$\forall\, D \in \mathcal{C}(X, \leq) \;:\; C^* \subseteq D \implies C^* = D$$

(0.27) Theorem: (viz. 691)
Hausdorff's Maximum Principle: Let $(X, \leq)$ be a partially ordered set, then there is a chain maximal $M \subseteq X$ in X (i.e. a maximal element of $\mathcal{C}(X, \leq)$ ordered under inclusion):

$$\forall C \in \mathcal{C}(X, \leq) \,:\, M \subseteq C \implies C = M$$

(0.28) Corollary: (viz. 694)
Lemma of Zorn: Let $(Z, \leq)$ be a partially ordered set, such that the following two properties are satisfied (1) $Z \neq \emptyset$ is non-empty and (2) every chain in Z has an upper bound, that is: For any $C \subseteq Z$ there is some $u \in Z$ such that for any $c \in C$ we have $c \leq u$. Then Z already has a maximal element, that is: for some $m \in Z$ any $z \in Z$ satisfies $m \leq z \implies m = z$. Formally:

$$\text{if } \forall C \in \mathcal{C}(Z, \leq)\, \exists u \in Z \,:\, \forall c \in C \,:\, c \leq u$$

$$\text{then } \exists m \in Z\, \forall z \in Z \,:\, m \leq z \implies z = m$$

(0.29) Remark:
We will mostly use the following special case of Zorn's Lemma: Let X be any set and $\mathcal{Z} \subseteq \mathcal{P}(X)$ be a non-empty $\mathcal{Z} \neq \emptyset$ family of subsets of X such that with any chain in $\mathcal{C} \subseteq \mathcal{Z}$ the union $\bigcup \mathcal{C} \in \mathcal{Z}$ is contained in $\mathcal{Z}$ as well, then $\mathcal{Z}$ has a maximal element: That is there is some $M \in \mathcal{Z}$ such that for any $Z \in \mathcal{Z}$ we have $M \subseteq Z \implies Z = M$. Formally again

$$\text{if } \forall \mathcal{C} \in \mathcal{C}(\mathcal{Z}, \subseteq) \,:\, \bigcup \mathcal{C} \in \mathcal{Z}$$

$$\text{then } \exists M \in \mathcal{Z}\, \forall Z \in \mathcal{Z} \,:\, M \subseteq Z \implies Z = M$$

Prob $(\mathcal{Z}, \subseteq)$ is a partially ordered set, such that $\mathcal{Z} \neq \emptyset$ if now $\mathcal{C} \subseteq \mathcal{Z}$ is a chain, then we let $U := \bigcup \mathcal{C}$. By assumption we have $U \in \mathcal{Z}$ and $C \subseteq U$ for any $C \in \mathcal{C}$ is clear. Then the lemma of Zorn yields $M \in \mathcal{Z}$.

We will use the lemma of Zorn to prove the existence of maximal ideals and modules with all kinds of properties. It can also be used to construct partial functions with maximal domain and so on. It is the single most powerful tool at or disposal! But though it is easy to use and very versatile (due to its generality) it only grants the existence of a maximal element. It does neither tell us how to find nor how to construct it. All we know, is that there *is* some.

(0.30) Theorem: (viz. 694)
Well-ordering Theorem: Let X be any set, then there is a total order $\leq$ on X that even satisfies the following *well-ordering* property: For any non-empty subset $A \subseteq X$, $A \neq \emptyset$ there is a *least element* $m \in A$, formally that is

$$\exists m \in A \;:\; \forall a \in A \;:\; m \leq a$$

(0.31) Remark:
These are the three basic theorems of set theory. And if we take a close look at the proofs [the reader is *not* required to do so, in order to be a good mathematician, but an understanding of the content of the theorems *is* required] we see that Hausdorff's maximum principle is derived from the axiom of choice, Zorn's lemma is derived from the maximum principle and the well-ordering theorem is derived from Zorn's lemma. We just want to sketch the idea that we can go full circle: The axiom of choice can be derived from the well-ordering theorem easily: Given an arbitrary collection $\mathcal{A} = \{ A_i \mid i \in I \}$ of non-empty sets $A_i \neq \emptyset$ we can construct a choice function in the following way: Let $A := \bigcup_i A_i$ and $X := \bigcup_i \{ i \} \times A_i \subseteq \mathcal{P}(I \times A)$ be the *disjoint union* of the A_i. Now install a well-ordering $\leq$ on X, then we may define a choice function $f : \mathcal{A} \to A$ by letting $f(A_i) := x_i$ where x_i is the minimum of the set $\{ i \} \times A_i \subseteq X$ under $\leq$, formally $(i, x_i) = \min(\{ i \} \times A_i)$. Therefore these three properties are equivalent on the basis of the other axioms of set theory. It is a different story, that they even are independent of the other axioms of set theory, that is they can neither be proved nor falsified. But this result requires much more effort in formal logic.

Comparing Cardinalities

(0.32) Lemma: (viz. 696)
Let X and Y be any two sets and let us agree two write $X \hookrightarrow Y$ iff there is an injective function f of the form $f : X \to Y$. Likewise we write $Y \twoheadrightarrow X$ iff there is a surjective function g of the form $g : Y \to X$. Finally we write $X \longleftrightarrow Y$ if there is a bijective function b of the form $b : X \to Y$. Using these notations we get the following statements

(i) For any two sets X and Y the properties $X \hookrightarrow Y$ and $Y \twoheadrightarrow X$ are equivalent.

(ii) For any two non-empty sets $X, Y \neq \emptyset$ we always have $X \hookrightarrow Y$ or $Y \hookrightarrow X$ (or both).

(iii) *Bernstein's Equivalence Theorem*: For any two sets X and Y we have the equivalence of

 (a) $X \longleftrightarrow Y$

 (b) $X \hookrightarrow Y$ and $Y \hookrightarrow X$

(0.33) Remark:
The benefit of these theorems is far reaching indeed: Note that we have defined the cardinal $|X|$ as $\{ Y \mid X \longleftrightarrow Y \}$. In particular $|\emptyset| = \emptyset$ (as $\emptyset$ does not admit a function, at all). And for any set with $1 \leq n \in \mathbb{N}$ elements $|X|$ contains all sets with exactly n elements.
Generally speaking $|X|$ is something like the equivalence class of X under the equivalence relation $\longleftrightarrow$, with the slight technical problem, that it only is a class, not a set. Thus $0 = \emptyset$ is the canonical representative of $|\emptyset|$ and n is the canonical representative of $|\{ 1, \ldots, n \}|$. Regardless, what is important is comparing cardinals: Recall that we have defined

$$
\begin{aligned}
|X| \leq |Y| \quad &:\Longleftrightarrow \quad X = \emptyset \text{ or } \exists\, f : X \to Y \text{ such that } f \text{ is injective} \\
|Y| \geq |X| \quad &:\Longleftrightarrow \quad X = \emptyset \text{ or } \exists\, g : Y \to X \text{ such that } g \text{ is surjective} \\
|X| = |Y| \quad &:\Longleftrightarrow \quad X = \emptyset = Y \text{ or } \exists\, b : X \to Y \text{ such that } f \text{ is bijective}
\end{aligned}
$$

That is $|X| \leq |Y|$ is another symbol for $X \hookrightarrow Y$, $|Y| \geq |X|$ is another symbol for $Y \twoheadrightarrow X$ and $|X| = |Y|$ is another symbol for $X \longleftrightarrow Y$. And by (0.32.(i)) $|X| \leq |Y|$ is equivalent to $|Y| \geq |X|$. So the usual notation for the inverse relation is respected. Now (0.32) is the reason that $\leq$ acts like a total order between the symbols $|X|$. That is for any sets X, Y and Z [this will be proved as (iv) in (0.32)] we have

$$\begin{gathered} |X| = |X| \\ |X| \leq |Y| \text{ or } |Y| \leq |X| \\ |X| \leq |Y| \text{ and } |Y| \leq |Z| \implies |X| \leq |Z| \\ |X| \leq |Y| \text{ and } |Y| \leq |X| \implies |X| = |Y| \end{gathered}$$

(0.34) Definition:
Recall that a set A is said to be **finite**, iff it only contains finitely many elements, that is iff it is empty or of the form $A = \{ a_1, \ldots, a_n \}$ for some $n \in \mathbb{N}$. Likewise A is said to be **infinite**, iff the natural numbers $\mathbb{N}$ fit into A injectively $\mathbb{N} \hookrightarrow A$. We will study different kinds of infinity: A is said to be **countably infinite**, iff it is of the form $A = \{ a_k \mid k \in \mathbb{N} \}$ (for some elements a_k with $a_k = a_l \implies k = l$). A set that is finite or countably infinite is said to be **countable** and if A is not countable, then it is called **uncountable**. We can put all this formally in a neat, compact form

$$\begin{aligned} A \text{ finite} &:\Longleftrightarrow \exists\, n \in \mathbb{N} : |A| = |1 \ldots n| \\ A \text{ infinite} &:\Longleftrightarrow |\mathbb{N}| \leq |A| \\ A \text{ countable} &:\Longleftrightarrow |A| \leq |\mathbb{N}| \\ A \text{ countably infinite} &:\Longleftrightarrow |A| = |\mathbb{N}| \\ A \text{ uncountable} &:\Longleftrightarrow |\mathbb{N}| < |A| \end{aligned}$$

(0.35) Lemma: (viz. 698)

(i) $|\mathbb{N}| = |\mathbb{Z}|$

(ii) $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$

(iii) $|\mathbb{N}| = |\mathbb{Q}|$

(iv) If $\Omega \neq \emptyset$ is a non-empty, countable index set and for any $i \in \Omega$ we are given a countable set A_i, then the union of all the A_i is countable again

$$\bigcup_{i \in \Omega} A_i \text{ is countable}$$

Nota of course the same is true, if we replace the word *countable* with *finite*, as the number of elements in the union cannot exceed the sum of the number of elements of the A_i.

(v) If $X \neq \emptyset$ is any non-empty set, then there is no surjective map of the form $X \to \mathcal{P}(X)$, in particular

$$|X| \ < \ |\mathcal{P}(X)|$$

We are about to study the peculiar behaviour of infinite sets. Countable infinity is the smallest kind of infinity, but even this is so much more then finiteness. Infinity is so many, it's hard to grasp: E.g. give a number to each atom in the universe (well, this is to say the section of the universe, we are able to see). Then remove all these numbers from $\mathbb{N}$. What will you get? Much the same thing! Even after removing all these numbers from $\mathbb{N}$, the rest still is infinite. The whole universe fits inside $\mathbb{N}$ and it does not even reduce the space remaining in there! Infinity is just so amazingly large. And there even are sets containing more elements: For any set X the power set $\mathcal{P}(X)$ is larger. So there's no stop in creating new levels of infinity!
Time to clean up this mess a little: We will present different characterisations of infinite sets, but we chose not to give one long list, but rather several short lists, sorted thematically. While the lemma of Zorn will be a major asset in our argumentations, cardinal arguments are rare, so we recommend to look up the following theorems, when needed. There is no inherent benefit in working through the theory. We also need a few preparations, before we can tackle infinity:

(0.36) Proposition: (viz. 701)
Let $\mathcal{A} = \{ A_i \mid i \in I \}$ and $\mathcal{B} = \{ B_k \mid k \in K \}$ be arbitrary collections of sets, such that the elements of $\mathcal{A}$ resp. of $\mathcal{B}$ are pairwise distinct. That is we have the implications

$$\begin{aligned} \forall\, i,j \in I \;\; : \;\; i \neq j \;\; &\Longrightarrow \;\; A_i \cap A_j = \emptyset \\ \forall\, k,l \in K \;\; : \;\; k \neq l \;\; &\Longrightarrow \;\; B_k \cap B_l = \emptyset \end{aligned}$$

Also suppose $\beta : I \longleftrightarrow K$ is a bijective map, such that for any $i \in I$ we have $|A_i| = |B_{\beta(i)}|$. Then the grand union of the sets $\mathcal{A}$ and $\mathcal{B}$ are of the same size, too - formally

$$|\bigcup_{i\in I} A_i| \;\; = \;\; |\bigcup_{k\in K} B_k|$$

(0.37) Definition:
Let $\mathcal{A} = \{ A_i \mid i \in I \}$ be arbitrary collections of sets again, that is $I \neq \emptyset$ is an arbitrary index set and for any $i \in I$ we consider another set A_i. Then the **disjoint union** of the A_i guarantees, that the contributing sets are pairwise disjoint. That is we define

$$\bigsqcup_{i\in I} A_i \;\; := \;\; \bigcup_{i\in I} A_i'$$

where $A_i' := \{ i \} \times A_i = \{ (i, a_i) \mid a_i \in A_i \}$. Nota It is clear, that $|A_i'| = |A_i|$, as $(i, a_i) \mapsto a_i$ is bijective and that for any $i, j \in I$ with $i \neq j$ we get $A_i' \cap A_j' = \emptyset$. Hence the name disjoint union is well-chosen.

Nota If we use this construction on a collection $\mathcal{A}$ of sets, without obvious index set I, we can use $\mathcal{A}$ as an index set, itself. That is for any $A \in \mathcal{A}$ we let $A' := \{ A \} \times A = \{ (A, a) \mid a \in A \}$. If we had $(X, x) \in A' \cap B'$ then $(X, x) \in A'$ implies $X = A$ and likewise $(X, x) \in B'$ implies $X = B$ such that $A = B$. Thus A' and B' are either identical or disjoint.

(0.38) Proposition: (viz. 701)

(i) Let X be an infinite set, then there is a partition $\mathcal{P} \subseteq \mathcal{P}(X)$ in the sense of (0.12) of X, such that any $P \in \mathcal{P}$ is countably infinite.

(ii) If X is an infinite set and $n \in \mathbb{N}$ with $n \geq 1$, then we can partition X into n subsets of equal size. That is here are subsets $A_1, \ldots, A_n \subseteq X$ such that (1) for any $i, j \in 1 \ldots n$ with $i \neq j$ we get $A_i \cap A_j = \emptyset$, (2) $X = A_1 \cup \cdots \cup A_n$ and (3) for any $i \in 1 \ldots n$ we have $|A_i| = |X|$.

(iii) If $X \neq \emptyset$ is any non-empty set, then the following four statements are equivalent

(a) X is infinite
(b) for any finite set F we get $|X| = |X \cup F|$
(c) for any finite set F we get $|X| = |X \setminus F|$
(d) for any subset $A \subseteq X$ we get $|X| = |A \sqcup X|$

(iv) If X is any set with $\#X \geq 2$, then the following four statements are equivalent

(a) X is infinite
(b) $|X| = |X^2|$
(c) there is some $n \in \mathbb{N}$ with $n \geq 2$ and $|X| = |X^n|$
(d) for any $n \in \mathbb{N}$ with $n \geq 1$ we have $|X| = |X^n|$

(v) If $X \neq \emptyset$ is any non-empty set, then the following four statements are equivalent

(a) X is infinite
(b) $|X| = |X \times \mathbb{N}|$
(c) The set X is if the same size, as the set of all finite tuples over X, formally that is

$$|X| \quad = \quad |\bigcup_{n=1}^{\infty} X^n|$$

(d) Let us denote by $\Omega(X) := \{ A \subseteq X \mid A \text{ is finite} \}$ the set of finite subsets of X. Then X and $\Omega(X)$ are of the same size, that is

$$|X| \quad = \quad |\Omega(X)|$$

(vi) Let $X, Y \neq \emptyset$ be non-empty sets, such that at least one of them is infinite. Then both, the disjoint union $X \sqcup Y$ and the cartesian product $X \times Y$ has as many elements, as the larger set of X or Y

$$|X \sqcup Y| \quad = \quad |X \times Y| \quad = \quad \max\{ |X|, |Y| \}$$

(vii) Let $I \neq \emptyset$ and X be any infinite set, with $|I| \leq |X|$. Suppose that for any $i \in I$ we are given a countable set A_i, then the union of the A_i cannot contain more elements than X, that is

$$|\bigcup_{i \in I} A_i| \quad \leq \quad |X|$$

0.6 A Primer on Classes

Let us begin this section with a list of the different axioms of set theory in commented form, hoping that the interested reader can thereby get an idea how Cantor's notion can be formalized. At times this will require to give two formulations: One of naive set theory and the other in (almost) formal logic. Later on we will sketch how to extend these axioms to handle classes:

(0.39) Remark: (ZFC)

(1) *Axiom of Extensionality:* Using Cantor's notion of a set it is clear that any sets X and Y are equal, if and only if they contain the same elements. That is why we can prove $X = Y$ by proving $X \subseteq Y$ and $Y \subseteq X$ separately. The first axiom formalizes this property, its formula reads

$$\forall X \, \forall Y \, : \, X = Y \iff \forall a \, \big(a \in X \iff a \in Y \big)$$

(2) *Axiom of Union:* Given any collection of sets $\mathcal{A} = \{ A_i \mid i \in I \}$ we often use the *grand union* $A = \bigcup_i A_i$ of these sets. Then a is an element of A if and only if $a \in A_i$ for some $i \in I$. The following axiom guarantees, that the set A truly exists

$$\forall \mathcal{A} \, \exists A \, : \, \forall a \, \big(a \in A \iff \exists A_i \, : \, (A_i \in \mathcal{A} \text{ and } a \in A_i) \big)$$

(3) *Axiom of Power Set:* For any set X there is a set containing all the subsets of X. This is called the *power set* $\mathcal{P}(X) = \{ A \mid A \subseteq X \}$ of X. The following axiom guarantees that the power set truly exists

$$\forall X \, \exists \mathcal{P} \, : \, \forall A \, \big(A \in \mathcal{P} \iff A \subseteq X \big)$$

thereby the inclusion of sets $A \subseteq X$ is an abbreviation for another formula: $A \subseteq X$ is defined, as $\forall a \, (a \in A \implies a \in X)$. For those versed in formal logic: We enrich the language of sets by picking up $\subseteq$ as a relation symbol and define its meaning by this formula.

(4) *Scheme of the Axioms of Separation:* Given a set X and a *predicate* φ on X (this is a function $\varphi : X \to \{ \text{true}, \text{ false} \}$ of X we would like to pick up the set $\{ x \in X \mid \varphi(x) \}$ that consists of all the elements $x \in X$ such that $\varphi(x) = \text{true}$. For Cantor the existence of this set is evident, in formal set theory the purpose of the list of axioms is to pin down what we take for granted. Thus for every *predicate* φ we allow

$$\forall X \, \exists A \, : \, \forall x \, \big(x \in A \iff \big(x \in X \text{ and } \varphi(x) \big) \big)$$

So what is a predicate in the context of this scheme of axioms? Of course φ is a formula in the formal language of sets. And this formula has to contain x as a *free* variable, that is x is a variable symbol that is not bound by a quantifier $\forall$ or $\exists$ already (a notion that is best defined by recursion on the setup of the formula). For this scheme we require that x is the one and only free variable symbol of φ.

(5) *Axiom of Infinity:* It is possible to construct the natural numbers $\mathbb{N}$ in terms of set theory: We start with $0 := \emptyset$ and iteratively define $n+1$ to be the set $n \cup \{n\}$. Then $\mathbb{N}$ is the set containing 0, $1 = 0+1$, $2 = 1+1$ and so on and it can be shown that any other set N that is generated by a succession function $N \to N : n \mapsto n^+$ from a starting element has an order-preserving bijection to $\mathbb{N}$. In this sense the natural numbers are unique up to isomorphy. The natural numbers are such a basic notion, that nobody would doubt them, but in formal set theory we have to guarantee their existence by an axiom:

$$\exists N \left(\emptyset \in N \text{ and } \forall n \left(n \in N \implies n \cup \{n\} \in N\right)\right)$$

In order to break this formula down into the language of formal set theory we have to make several replacements: The empty set $\emptyset$ is defined by $E = \emptyset \iff \forall x (x \in \emptyset \iff x \neq x)$ Thus instead of $\emptyset \in N$ we would have to write $\exists E (E = \emptyset \text{ and } E \in N)$. The existence of $\emptyset$ is guaranteed by (4), just take the predicate $\varphi = (x \neq x)$. So it remains to define $n^+ = n \cup \{n\}$: Clearly $a \in n^+$ iff $a \in n$ or $a = n$. Thus we let $s = n^+ \iff \forall a (a \in n \text{ or } a = n)$. Therefore n^+ needs to be replaced by $\exists s (s = n^+ \text{ and } s \in N)$. The resulting formula is far too long to be captured in one line and hence we will abstain from providing it here.

(6) *Scheme of the Axioms of Replacement:* If $f : X \rightarrowtail Y$ is a partial function and $A \subseteq X$ is a subset of X, then we would like to map A (that is the part of A inside the domain of f) to Y. If $a \in A$ is mapped under f then the element $b = f(a) \in Y$ is uniquely determined. Therefore we will get a subset $B = f(A) = \{ f(a) \mid a \in A \cap \mathrm{dom}(f) \} \subseteq Y$. Let us make the existence of $f(A)$ an axiom:

$$\forall f \left(f : X \rightarrowtail Y \implies \forall A \exists B \forall b \left(b \in B \iff b \in f(A)\right)\right)$$

$$\text{where} \quad b \in f(A) \quad :\iff \quad \exists a \left(a \in A \text{ and } b = f(a)\right)$$

It requires some effort to formulate this in the language of sets. First of all we have to replace the partial function f: Let φ be a formula in the language of sets having the the free variables x and y [refer to (4) for this]. If now a and b are any variable symbols, then $\varphi(x : a, y : b)$ denotes the formula where every free occurrence of x is replaced by a and any free occurence of y is replaced by b. We now recall how we introduced functions as sets: We defined $b = f(a)$ by afb. Thus we replace $b = f(a)$ by $\varphi(x : a, y : b)$. Consequently $f : X \rightarrowtail Y$ has to be replaced by

$$\forall a \forall b_1 \forall b_2 \left(\left(\varphi(x : a, y : b_1) \text{ and } \varphi(x : a, y : b_2)\right) \implies b_1 = b_2\right)$$

It remains to replace the quantifier $\forall f$, as we replaced f by a formula φ. Hence we take this formula as an axiom for every formula φ that has the free variables x, y and $s_1, \ldots, s_n$ ($n \in \mathbb{N}$) but no others. Then we replace $\forall f$ by $\forall s_1 \ldots \forall s_n$ and are finally done.

(7) *Axiom of Foundation:* Cantor would say that no set can satisfy $X \in X$, by the following reasoning: In order to build up the set X we need to know all its elements. So X cannot be on of its own elements, since by the time we think of the set X the element X is incomplete. For the same reason there can be no circle of sets $X_1 \in X_2$, $X_2 \in X_3$ and so on $X_{n-1} \in X_n$ with $X_n \in X_1$ again.

In formal set theory one usually takes a little stronger property to be an axiom: Every non-empty set X contains an element d, that is disjoint to X, as a formula:

$$\forall X \left(X \neq \emptyset \implies \exists d \left(d \in X \text{ and } d \cap X = \emptyset \right) \right)$$

In the formal language we only have to make little adjustments: $X \neq \emptyset$ needs to be reformulated as $\exists u\, u \in X$ and $d \cap X = \emptyset$ has to be replaced by $\forall v \left(v \in x \text{ and } v \in X \implies v \neq v \right)$. It is easy to deduce the non-existence of circles from this axiom (see below). And using the axiom of choice we can also deduct this formula from the non-existence of circles of sets.

Prob Suppose we had a circle of sets $x_1, \ldots, x_n$ such that $x_k \in x_{k+1}$ and $x_n \in x_1$. Then we consider $X := \{ x_1, \ldots, x_n \}$ and choose some $d \in X$ such that $d \cap X = \emptyset$. By construction we have $d = x_k$ for some $k \in 1 \ldots n$. Thus $x_{k-1} \in d$ or $x_n \in d$ for $k = 1$. That is $x_i \in d$ for some $i \in 1 \ldots n$. But then $x_i \in d \cap X$ in contradiction to $d \cap X = \emptyset$.

(8) *Axiom of Choice:* This has often been stated: Given an arbitrary collection of sets $\mathcal{A} = \{ A_i \mid i \in I \}$ such that $A_i \neq \emptyset$ is non-empty (for any $i \in I$) there is a set $A = \{ a_i \mid i \in I \}$ such that for any $i \in I$ the element a_i is taken from $a_i \in A_i$. We say that A is a *choice from* $\mathcal{A}$.

In fact it suffices to claim a little less: If $\mathcal{P}$ is a partition of some set X then there is a set $A \subseteq X$ such that for any $a \in A$ there is exactly one $P \in \mathcal{P}$ such that $a \in P$ (see below). We will now formalize this property as an axiom:

$$\forall \mathcal{P} \left(\mathcal{P} \text{ partition} \implies \exists A \ : A \text{ choice from } \mathcal{P} \right)$$

Hereby "$\mathcal{P}$ partition" abbreviates a formula in the language of sets, namely $\emptyset \notin \mathcal{P}$ and $(\forall P \forall Q \ldots)$ where $\ldots$ is given to be the following formula

$$P \in \mathcal{P} \text{ and } Q \in \mathcal{P} \text{ and } \exists x \left(x \in P \text{ and } x \in Q \right) \implies P = Q$$

And likewise "A choice from $\mathcal{P}$" abbreviates another formula, this time the abbreviated formula is

$$\forall P \left(P \in \mathcal{P} \implies \exists!\, a \left(a \in A \text{ and } a \in P \right) \right)$$

Prob Let us define $P_i := \{ i \} \times A_i$ and $X := \bigcup P_i$ Then it is clear that $\mathcal{P} := \{ P_i \mid i \in I \}$ is a partition of X. Thus there is some $P \subseteq X$ such that for any $p \in P$ there is a unique $P_i \in \mathcal{P}$ with $p \in P_i$. By construction p is of the form $p = (i, a)$ for some $a \in A_i$. Now define $\pi : X \to \bigcup_i A_i$ by $(i, a) \mapsto a$. Then $A := \pi(P)$ is a choice from $\mathcal{A}$.

Intuitively speaking classes are collections of sets that are just too large to be a set themselves. E.g. if we denote $\mathcal{U}$ the collection of *all* sets (sometimes also called the *universe*) and would think that this could be a set, then we would have $\mathcal{U} \in \mathcal{U}$, which we shun. As we wish to address such constructions, we need a new term for these, in order to avoid contradictions. This new term is **class**, that's all. In fact there are classes, that can well be sets, these classes are called *small*, but the interesting classes are not.

Warning: The rest of this section will advance set-theory by introducing classes, as a second, fundamental concept. This will definitely not be needed prior to chapter 11 where we proceed on to categorial algebra. And even there, a naive understanding of classed is all that is required. Do not venture on with this section, unless you have a solid working knowledge of set theory and feel comfortable with the axioms of ZFC. And if you are interested in standard algebra only, skip this section entirely. You will *not* miss a single thing.

From a formal point of view we extend the language of sets (with only one sort of variable symbols, which we interpret as sets) to a language of sets and classes (with two sorts of variable symbols, one for sets and one for classes). Most textbooks try to avoid this by introducing two predicate symbols one saying *I am a set* and the other saying *I am a class*, but accepting the two sorts is the natural way to go. Thus in this two-sorted language we will have separate quantifiers for the different sorts:

	universal quantifier	existential quantifier
sets	$\forall_s$	$\exists_s$
classes	$\forall_c$	$\exists_c$

For example the formula $\forall_s X \, \exists_c \mathcal{C} : X = \mathcal{C}$ says: For every set X there is a class $\mathcal{C}$ that is equal to X. This will even be the first of our axioms for classes. So here comes the rest: A commented list of (NBG) !! NBG axioms !!

Chapter 1

Groups and Rings

1.1 Defining Groups

The most familiar (and hence easiest to understand) objects of algebra are rings. And of these the easiest example are the integers $\mathbb{Z}$. On these there are two operations: an addition $+$ and a multiplication $\cdot$. Both of these operations have familiar properties (associativity for example). So we first study objects with a single operation $\circ$ only - monoids and groups - as these are a unifying concept for both addition and multiplication. However our aim solely lies in preparing the concepts of rings and modules, so the reader is asked to venture lightly over problems within this section until he has reached the later sections of this chapter.

(1.1) Definition:
Let $G \neq \emptyset$ be any non-empty set and $\circ$ a *binary operation* on G, i.e. $\circ$ is a mapping of the form $\circ : G \times G \to G : (x,y) \mapsto xy$. Then the ordered pair $(G,\circ)$ is said to be a **monoid** iff it satisfies the following properties

(A) $\forall\, x,y,z \in G \;:\; x(yz) \;=\; (xy)z$

(N) $\exists\, e \in G \;\; \forall\, x \in G \;:\; xe \;=\; x \;=\; ex$

Note that this element $e \in G$ whose existence is required in (N) then already is uniquely determined (see below). It is said to be the **neutral element** of G. And therefore we may define: A monoid $(G,\circ)$ is said to be a **group** iff any element $x \in G$ has an **inverse element** $y \in G$, that is iff

(I) $\forall\, x \in G \;\; \exists\, y \in G \;:\; xy \;=\; e \;=\; yx$

Note that in this case the inverse element y of x is uniquely determined (see below) and we hence write $x^{-1} := y$. Finally a monoid (or group) $(G,\circ)$ is said to be **commutative** iff it satisfies the property

(C) $\forall\, x,y \in G \;:\; xy \;=\; yx$

(1.2) Remark:

- We have to append some remarks here: First of all we have employed a function $\circ : G \times G \to G$. The image $\circ(x,y)$ of the pair $(x,y) \in G \times G$ has been written in an unfamiliar way however

$$xy \;:=\; \circ(x,y)$$

If you have never seen this notation before it may be somewhat startling, in this case we would like to reassure you, that this actually is nothing new - just have a look at the examples further below. Yet this notation has the advantage of restricting itself to the essential. If we had stuck to the classical notation such terms would be by far more obfuscated. E.g. let us rewrite property (A) in classical terms

$$\circ\Big(x, \circ(y,z)\Big) \;=\; \circ\Big(\circ(x,y), z\Big)$$

- It is easy to see that the neutral element e of a monoid $(G,\circ)$ is uniquely determined: Suppose that another element $f \in G$ would satisfy $\forall\, x \in G : xf = x = fx$, then we would have $ef = e$ by letting $x = e$. But as e is a neutral element we have $ef = f$ by (N) applied with $x = f$. And hence $e = f$ are equal, i.e. e is uniquely determined. Hence in the following we will reserve the letter e for the neutral element of the monoid regarded *without specifically mentioning it*. In case we apply several monoids at once, we will name the respective neutral elements explicitly.

- Property (A) is a very important one and hence it has a name of its own: **associativity**. A pair $(G,\circ)$ that satisfies (A) only also is called a **groupoid**. We will rarely employ these objects however.

- Suppose $(G,\circ)$ is a monoid with the (uniquely determined) neutral element $e \in G$. And suppose $x \in G$ is some element of G, that has an inverse element. Then this inverse is uniquely determined: Suppose both y and $z \in G$ satisfy $xy = e = yx$ and $xz = e = zx$. Then the asociativity yields $y = z$, as we may compute

$$y \;=\; ye \;=\; y(xz) \;=\; (yx)z \;=\; ez \;=\; z$$

- Another important consequence of the associativity is the following: Consider finitely many elements $x_1, \ldots, x_n \in G$ (where $(G,\circ)$ is a groupoid at least). Then any application of parentheses to the product $x_1x_2\ldots x_n$ produces the same element of G. As an example consider

$$x_1(x_2(x_3x_4)) \;=\; x_1((x_2x_3)x_4) \;=\; (x_1(x_2x_3))x_4 \;=\; ((x_1x_2)x_3)x_4$$

 In every step of these equalities we have only used the associativity law (A). The remarkable fact is that *any* product of *any* n elements (here $n = 4$) only depends on the order of the elements, not on the bracketing. Hence it is costumary to omit the bracketing altogether

$$x_1x_2\ldots x_n \;:=\; \Big((x_1x_2)\ldots\Big)x_n \;\in\; G$$

 And any other assignment of pairs (without changing the order) to the elements x_i would yield the same element as $x_1x_2\ldots x_n$. A formal version of this statement and its proof are given in section 15.2 of this book. The proof clearly will be done by induction on $n \geq 3$, the foundation of the induction precisely is the law of associativity.

- Suppose $(G,\circ)$ is any groupoid, $x \in G$ is an element and $1 \leq k \in \mathbb{N}$, then we abbreviate the k-nary product of x by x^k, i.e. we let

$$x^k \;:=\; xx\ldots x \quad (k - \text{times})$$

If $(G, \circ)$ even is a monoid (with neutral element e) it is customary to define $x^0 := e$. Thus in this case $x^k \in G$ is defined for all $k \in \mathbb{N}$. Now suppose that x even is invertible (e.g. if $(G, \circ)$ is a group), then we may even define $x^k \in G$ for any $k \in \mathbb{Z}$. Suppose $1 \leq k \in \mathbb{N}$, then

$$x^{-k} \;:=\; \left(x^{-1}\right)^k$$

- In a commutative groupoid $(G, \circ)$ we may even change the order in which the $x_1, \ldots, x_n \in G$ are multiplied. I.e. if we are given a bijective map $\sigma : 1 \ldots n \longleftrightarrow 1 \ldots n$ on the indexes $1 \ldots n$ we get

$$x_{\sigma(1)} x_{\sigma(2)} \ldots x_{\sigma(n)} \;=\; x_1 x_2 \ldots x_n$$

 The reason behind this is the following: Any permutation σ can be decomposed into a series of transpositions (this is intuitively clear: We can generate any order of n objects by repeatedly interchanging two of these objects). In fact any transposition can be realized by interchanging adjacent objects only. But any transposition of adjacent elements is allowed by property (C). A formal proof of this reasoning will be presented in section 15.2 again.

(1.3) Example:

- The most familiar example of a (commutative) monoid are the natural numbers under addition: $(\mathbb{N}, +)$. Here the neutral element is given to be $e = 0$. However $1 \in \mathbb{N}$ has no inverse element (as for any $a \in \mathbb{N}$ we have $a + 1 > 0$) and hence $(\mathbb{N}, +)$ is no group.

- The integers however are a (commutative) group $(\mathbb{Z}, +)$ under addition. The neutral element is zero again $e = 0$ and the inverse element of $a \in \mathbb{Z}$ is $-a$. Thus $\mathbb{N}$ is contained in a group $\mathbb{N} \subseteq \mathbb{Z}$.

- Next we regard the non-zero rational numbers $\mathbb{Q}^* := \{\, a/b \mid 0 \neq a, b \in \mathbb{Z} \,\}$. These form a group under multiplication $(\mathbb{Q}^*, \cdot)$. The neutral element is given to be $e = 1/1$ and the inverse of some $a/b \in \mathbb{Q}^*$ is its sweep break $(a/b)^{-1} = b/a$.

- Consider any non-empty set $X \neq \emptyset$. Then the set of maps from X to X, which (as always) we denote by $\mathcal{F}(X) := \{\, \sigma \mid \sigma : X \to X \,\}$, becomes a monoid under the composition of maps $(\mathcal{F}(X), \circ)$ (as the composition of functions is associative). The neutral element is the identity map $e = \mathbb{1}_X$ which is given to be $\mathbb{1}_X : x \mapsto x$.

- Consider any non-empty set $X \neq \emptyset$ again. Then $S_X := \{\, \sigma : X \to X \mid \sigma \text{ bijective} \,\} \subseteq \mathcal{F}(X)$ the set of bijective maps on X even becomes a group under the composition of maps $(S_X, \circ)$. The neutral element is the identity map $e = \mathbb{1}_X$ again and the inverse of $\sigma \in S_X$ is the inverse function σ^{-1}. This will be continued in the next section.

- $(\diamondsuit)$ A special case of the above is $\mathrm{gl}_n(E) := \{\, A \in \mathrm{mat}_n(E) \mid \det(A) \neq 0 \,\}$ the set of invertible $(n \times n)$-matrices over a field $(E, +, \cdot)$. This is a group $(\mathrm{gl}_n(E), \cdot)$ under the multiplication $\cdot$ of matrices. Symmetries in E^n are subgroups of $\mathrm{gl}_n(E)$ and representation theory will be concerned with regarding *any* group G as some subgroup of $\mathrm{gl}_n(E)$.

(1.4) Remark:
Consider a finite groupoid $(G, \circ)$, that is the set $G = \{ x_1, \ldots, x_n \}$ is finite. Then the composition $\circ$ can be given by a table of the following form

$\circ$	x_1	x_2	$\ldots$	x_n
x_1	x_1x_1	x_1x_2	$\ldots$	x_1x_n
x_2	x_2x_1	x_2x_2	$\ldots$	x_2x_n
$\vdots$	$\vdots$	$\vdots$		$\vdots$
x_n	x_nx_1	x_nx_2	$\ldots$	x_nx_n

Such a table is also known as the **Cayley diagram** of G. As an example consider a set with 4 elements $K := \{ e, x, y, z \}$, then the following diagram determines a group structure $\circ$ on K [what we do not want to prove here, but you can easily see, that K is commutative and $k^2 = e$ and hence $k^{-1} = k$ for any $k \in K$]. This group $(K, \circ)$ is called the *Klein 4-group*.

$\circ$	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

(1.5) Proposition: (viz. 710)
Let $(G, \circ)$ be any group (with neutral element e), x, $y \in G$ be any two elements of G and k, $l \in \mathbb{Z}$. Then we obtain the following identities

$$\begin{aligned} e^{-1} &= e \\ \left(x^{-1}\right)^{-1} &= x \\ \left(xy\right)^{-1} &= y^{-1}x^{-1} \\ x^k x^l &= x^{k+l} \\ \left(x^k\right)^l &= x^{kl} \end{aligned}$$

In particular the inversion $i : G \longleftrightarrow G : x \mapsto x^{-1}$ of elements is a self-inverse, bijective mapping $i = i^{-1}$ on the group G. If now $xy = yx$ do commute then for any $k \in \mathbb{Z}$ we also obtain

$$xy = yx \quad \Longrightarrow \quad (xy)^k = x^k y^k$$

(1.6) Definition:
If $(G, \circ)$ and $(H, \circ)$ are any two groups, whose neutral elements are $e \in G$ and $f \in H$ respectively, then a map $\varphi : G \to H$ is said to be a **homomorphism of groups** or *group-homomorphism*, iff it satisfies

$$\forall\, x, y \in G \quad \text{we get} \quad \varphi(xy) \;=\; \varphi(x)\varphi(y)$$

And in this case φ already links the neutral elements and maps inverse elements to the inverse, that is it satisfies $\varphi(e) = f$ and [the proof will be given shortly]

$$\forall\, x \in G \quad \text{we get} \quad \varphi(x^{-1}) \;=\; \varphi(x)^{-1}$$

Let us introduce the set of all group-homomorphisms from G to H, which we will denote as

$$\mathrm{ghom}(G,H) \;:=\; \{\, \varphi : G \to H \mid \forall\, x,y \in G : \varphi(xy) = \varphi(x)\varphi(y) \,\}$$

Prob clearly $\varphi(e) = \varphi(ee) = \varphi(e)\varphi(e)$ but as H is a group we may multiply by $\varphi(e)^{-1}$ to find $f = \varphi(e)$. Therefore we have $f = \varphi(e) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1})$. And likewise we get $f = \varphi(x^{-1})\varphi(x)$ and hence $\varphi(x^{-1}) = \varphi(x)^{-1}$ as we had claimed before.

(1.7) Proposition: (viz. 712)
Let $(G,\circ)$ be a group with neutral element $e \in G$, then a subset $P \subseteq G$ is said to be a **subgroup** of G (written as $P \leq_{\mathrm{g}} G$) iff it satisfies

$$\begin{aligned} e \quad &\in \quad P \\ x,y \in P \quad &\Longrightarrow \quad xy \in P \\ x \in P \quad &\Longrightarrow \quad x^{-1} \in P \end{aligned}$$

In other words $P \subseteq G$ is a subgroup of G iff it is a group $(P,\circ)$ under the operation $\circ$ inherited from G. And in this case we obtain an equivalence relation on G by letting (for any x, $y \in G$)

$$x \sim y \quad :\Longleftrightarrow \quad y^{-1}x \in P$$

And for any $x \in G$ the equivalence class of x is thereby given to be the **coset** $xP := [x] = \{\, xp \mid p \in P \,\}$. We thereby define the **index** $[G : P]$ of P in G to be the following cardinal number

$$\begin{aligned} G\big/_P \;&:=\; G\big/_\sim \\ [\,G : P\,] \;&:=\; \left|G\big/_P\right| \end{aligned}$$

And thereby we finally obtain the following identity of cardinals which is called the *Theorem of Lagrange* (and which means, that there is a bijective map $G \longleftrightarrow (G/P) \times P$)

$$|G| \;=\; [\,G : P\,] \cdot |P|$$

(1.8) Proposition: (viz. 712)
Let $(G,\circ)$ be any monoid with neutral element e and $X \subseteq G$ be any subset of G. Then the intersection of all submonoids of G that contain X is a submonoid of G again

$$\langle X \rangle_{\mathrm{o}} \;:=\; \bigcap \{\, P \leq_{\mathrm{o}} G \mid X \subseteq P \,\} \quad \leq_{\mathrm{o}} \quad G$$

We call $\langle X \rangle_o$ the monoid **generated** by $X \subseteq G$. And letting $X_e := X \cup \{ e \}$ we can even give an explicit description of $\langle X \rangle_o$ to be the following set

$$\langle X \rangle_o \quad = \quad \{ x_1 x_2 \dots x_n \mid n \in \mathbb{N},\, x_1, \dots, x_n \in X_e \}$$

If G even is a group, then we can regard the intersection of all subgroups of G that contain X and this is a subgroup of X again

$$\langle X \rangle_g \quad := \quad \bigcap \{ P \leq_o G \mid X \subseteq P \} \quad \leq_g \quad G$$

Likewise we call $\langle X \rangle_g$ the group **generated** by $X \subseteq G$. And letting $X_\pm := X \cup \{ e \} \cup \{ x^{-1} \mid x \in X \}$ we can even give an explicit description of $\langle X \rangle_g$ to be the following set

$$\langle X \rangle_g \quad = \quad \{ x_1 x_2 \dots x_n \mid n \in \mathbb{N},\, x_1, \dots, x_n \in X_\pm \}$$

(1.9) Proposition: (viz. 713)
If $(G, \circ)$ is a group and $x \in G$ is any element of G, then the above proposition tells us that the subgroup generated by x is given to be

$$\langle x \rangle_g \quad = \quad \left\{ x^k \mid k \in \mathbb{Z} \right\}$$

If now G is *finite*, that is $n := \#G \in \mathbb{N}$, then $\langle x \rangle_g$ (being a subset) is finite too. In particular we may define the **order** of x to be number of elements of $\langle x \rangle_g$. And thereby we find

$$\operatorname{ord}(x) \quad := \quad \#\langle x \rangle_g \quad = \quad \min \left\{ 1 \leq k \in \mathbb{N} \mid x^k = e \right\}$$

That is $k = \operatorname{ord}(x)$ is the *minimal* number $1 \leq k \in \mathbb{N}$ such that $x^k = e$ and this k divides n. That is for a finite group G and any element $x \in G$ we will always have

$$\operatorname{ord}(x) \quad | \quad \#G$$

And from this we conclude another *theorem of Lagrange:* In particular, if G is finite, containing $n := \#G$ elements, then any element $x \in G$ satisfies $x^n = e$, formally we get

$$x^{\#G} \quad = \quad e$$

1.2 Permutations

In this section we will study the most important and most general example of groups: permutations. Permutation groups will not become important until we reach determinants in chapter 4. So a novice might well skip the entire section and return to it only later. In fact we even recommend this approach, as we deem the basics of ring theory to be easier to understand, than the basics of group theory. Also we will use some notation (namely products and the faculty) that will only be introduced in sections 1.3 and 1.5 respectively.
Later in section 9.2 we will introduce group actions, that are a generalization of the permutation action. Also permutations are used to study conjugation in a group and they are occasionally useful in other areas as well. In fact they will be applied in Galois, representation and invariant theory.

(1.10) Definition: (viz. 714)
If $X \neq \emptyset$ is any non-empty set then we define the group S_X of **permutations** of X to be the set of all bijective maps on X, that is

$$S_X \;:=\; \{\, \sigma : X \to X \mid \sigma \text{ is bijective} \,\}$$

Thereby S_X truly becomes a group $(S_X, \circ)$ under usual the composition $\circ$ of functions. An in case of $X = 1 \ldots n$ we will write

$$S_n \;:=\; \{\, \sigma : (1 \ldots n) \to (1 \ldots n) \mid \sigma \text{ is bijective} \,\}$$

(1.11) Remark:
If $\emptyset \neq X \subseteq Y$ is a non-empty subset of some set Y, then it is clear that the permutations on X can be regarded as a subset of the permutations on Y. That is we get the following monomorphism of groups:

$$S_X \hookrightarrow S_Y \;:\; \pi \mapsto \overline{\pi}$$

where $\overline{\pi} : Y \to Y$ is defined by $\overline{\pi}(x) := \pi(x)$ for any $x \in X$ and $\overline{\pi}(y) := y$ for any $y \in Y \setminus X$. The image if this monomorphism is just the set of all $\sigma \in S_Y$ that fix all the elements of $Y \setminus X$, formally again:

$$S_X \longleftrightarrow \{\, \sigma \in S_Y \mid \forall\, y \in Y \setminus X : \sigma(y) = y \,\}$$

(1.12) Proposition: (viz. 714)

(i) If X is a finite set, $n := \#X \in \mathbb{N}$then the group $(S_X, \circ)$ is finite again, in fact it contains precisely $n!$ elements, formally that is

$$\#S_X \;=\; (\#X)!$$

(ii) Fix any $1 \leq n \in \mathbb{N}$ and [the set $X := 1 \ldots (n+1)$] and denote the subgroup of all permutations $\sigma \in S_{n+1} = S_X$ that fix $n+1$ by

$$S'_n \;:=\; \{\, \sigma \in S_{n+1} \mid \sigma(n+1) = n+1 \,\}$$

And for any $k \in 1 \ldots (n+1)$ denote $\tau_k := (k\ n+1)$ the *transposition* of k and $n+1$, i.e. the permutation that only interchanges these two numbers. Then we will prove that the following subsets of S_{n+1} are identical

$$\begin{aligned} \tau_k S'_n &:= \{\, \tau_k \pi \mid \pi \in S'_n \,\} \\ &= \{\, \sigma \in S_{n+1} \mid \sigma(n+1) = k \,\} \end{aligned}$$

And thereby S_{n+1} can be written as the following disjoint union (*disjoint* is to say, that for any $i \neq j \in 1 \ldots (n+1)$ we have $\tau_i S'_n \cap \tau_j S'_n = \emptyset$)

$$S_{n+1} := \bigcup_{k=1}^{n+1} \tau_k S'_n$$

(iii) If $(G, \circ)$ is any group, then G can be embedded into $(S_G, \circ)$. To be precise the following map is well-defined and injective

$$L : G \hookrightarrow S_G : g \mapsto L_g$$

$$L_g : G \to G : x \mapsto gx$$

and a homomorphism of groups, that is: $L_e = \mathbb{1}_G$ and for any $g, h \in G$ we get $L_{gh} = L_g L_h$. NOTA in this sense the permutation groups S_X are the most general groups whatsoever.

(1.13) Definition:
Fix a non-empty set $X \neq \emptyset$ and consider the permutation group $(S_X, \circ)$. For any permutation $\sigma \in S_X$ and any $x \in X$, we define the **fixed point** set $\mathrm{fix}(\sigma)$ of σ and its complement $\mathrm{dom}(\sigma)$ is called the **domain** of σ. Also $\mathrm{cyc}(\sigma, x)$ is called the **cycle** of x under σ and $\ell(\sigma, x)$ is said to be the **length** of that cycle.

$$\begin{aligned} \mathrm{fix}(\sigma) &:= \{\, x \in X \mid \sigma(x) = x \,\} \\ \mathrm{dom}(\sigma) &:= \{\, x \in X \mid \sigma(x) \neq x \,\} \\ \mathrm{cyc}(\sigma, x) &:= \left\{\, \sigma^k(x) \mid k \in \mathbb{N} \,\right\} \\ \ell(\sigma, x) &:= \#\,\mathrm{cyc}(\sigma, x) \end{aligned}$$

(1.14) Proposition: (viz. 715)
Fix a non-empty set $X \neq \emptyset$ and consider the permutation group $(S_X, \circ)$. Then, for any permutations ϱ and $\sigma \in S_X$ and any $x \in X$ we find the following statements

(i) If $n := \#X < \infty$ is finite, then the length $\ell(\sigma, x)$ if finite, too. More precisely the length of the cycle of x under σ cannot exceed the order of σ, and therefore

$$\ell(\sigma, x) \;\leq\; \mathrm{ord}(\sigma) \;\leq\; n!$$

(ii) The fixed points and domain of σ are stable under σ. That is for any $x \in \mathrm{fix}(\sigma)$ we find $\sigma(x) \in \mathrm{fix}(\sigma)$ again. Likewise for any $x \in \mathrm{dom}(\sigma)$ we find $\sigma(x) \in \mathrm{dom}(\sigma)$. In fact we even find

$$\sigma\big(\mathrm{fix}(\sigma)\big) \;=\; \mathrm{dom}(\sigma)$$

$$\sigma\big(\mathrm{dom}(\sigma)\big) \;=\; \mathrm{dom}(\sigma)$$

In particular, if $x \in \mathrm{dom}(\sigma)$ is contained in the domain of σ, then $\sigma^k(x)$ is contained in the domain of σ, for any power $k \in \mathbb{N}$, such the entire cycle of x is contained in the domain of σ

$$\mathrm{cyc}(\sigma, x) \;\subseteq\; \mathrm{dom}(\sigma)$$

(iii) If ϱ and σ share a common domain $D \subseteq X$ and agree on D, then they already are equal. Formally that is the following equivalence of

$$\left.\begin{array}{l} D := \mathrm{dom}(\varrho) = \mathrm{dom}(\sigma) \\ \forall\, x \in D \;:\; \varrho(x) = \sigma(x) \end{array}\right\} \quad\Longleftrightarrow\quad \varrho \;=\; \sigma$$

(iv) If the domains of ϱ and σ are disjoint, then ϱ and σ commute. That is we have the implication

$$\mathrm{dom}(\varrho) \cap \mathrm{dom}(\sigma) \;=\; \emptyset \quad\Longrightarrow\quad \varrho\sigma \;=\; \sigma\varrho$$

(1.15) Definition:
Fix $n \in \mathbb{N}$ with $n \geq 1$ and consider an ℓ-tuple $(i_1, \ldots, i_\ell)$ of natural numbers $i_k \in 1 \ldots n$ that are pariwise distinct (that is $i_j = i_k \implies j = k$). Then the tuple $(i_1, \ldots, i_\ell)$ gives rise to a permutation $\zeta \in S_n$ by

$$\zeta(a) \;:=\; \begin{cases} a \text{ if } a \in (1 \ldots n) \setminus \{\, i_1, \ldots, i_\ell \,\} \\ i_{k+1} \text{ if } a = i_k \text{ for some } k \in 1 \ldots \ell - 1 \\ i_1 \text{ if } a = i_\ell \end{cases}$$

This permutation $\zeta \in S_n$ is called a **cycle** of **length** ℓ and (by slight abuse of notation, as n is not specified) we will denote this cycle by the symbol

$$(i_1\; i_2\; \ldots\; i_\ell) \;:=\; \zeta$$

A cycle of length 2 is said to be a **transposition** of S_n. And by definition it interchanges two numbers $i \neq j$. That is, if $\tau = (i\; j)$ then $\tau(i) = j$ and $\tau(j) = i$ and $\tau(a) = a$ for any other $a \in 1 \ldots n$.

(1.16) Remark: (viz. 716)

- The notation of cycles is ambigious as it is of no effect with which element the cycle starts, as long as the ordering of elements is not changed. That is $(i_1\; i_2\; \ldots\; i_\ell)$ and $(i_2\; i_3\; \ldots\; i_\ell\; i_1)$ and so on until $(i_\ell\; i_1\; i_2\; \ldots\; i_{\ell-1})$ all yield the same permutation. In particular we have $(i\; j) = (j\; i)$ for any transposition.

- Any cycle ζ can be written as a composition of transpositions. Let us be explicit: Given the cycle $(i_1\ i_2\ \ldots\ i_\ell)$ we can rewrite this one, in the following form

$$(i_1\ i_2\ \ldots\ i_\ell) \quad = \quad (i_1\ i_\ell)(i_1\ i_{\ell-1})\ldots(i_1\ i_2)$$

- Any transposition can be written as a composition of transpositions of adjacent elements. To be precise given any $i, j \in 1\ldots n$ with $i < j$ we can rewrite

$$(i\ \ j) \ = \ (i\ \ i+1)(i+1\ \ i+2)\ldots(j-1\ \ j)(j-2\ \ j-1)\ldots(i\ \ i+1)$$

- If $\zeta = (i_1\ i_2\ \ldots\ i_\ell) \in S_n$ is a cycle of length ℓ, then for any other permutation $\sigma \in S_n$ the conjugate $\sigma\zeta\sigma^{-1}$ is another cycle of length ℓ. In fact we get

$$\sigma\zeta\sigma^{-1} \quad = \quad (\sigma(i_1)\ \ \sigma(i_2)\ \ \ldots\ \ \sigma(i_\ell))$$

(1.17) Proposition: (viz. 717)
Fix $n \in \mathbb{N}$ with $n \geq 1$ and consider the perumtation group $(S_n, \circ)$. If now $\sigma \in S_n$ is any permutation with $\sigma \neq \mathbb{1}$ then the following five statements are equivalent:

(a) σ is a **cycle**, that is there are some $\ell \geq 2$ and some pairwise distinct $i_1, i_2, \ldots, i_\ell \in 1\ldots n$ [which is to say is $i_j = i_k \implies j = k$] such that

$$\sigma \quad = \quad (i_1\ i_2\ \ldots\ i_\ell)$$

(b) Any two elements $a, b \in \mathrm{dom}(\sigma)$ in the domain of σ are linked in the following sense: There is some $k \in \mathbb{N}$ such that $b = \sigma^k(a)$.

(c) For any element $i \in \mathrm{dom}(\sigma)$ the domain of σ already is generated by the orbit of i under σ, that is

$$\mathrm{dom}(\sigma) \quad = \quad \left\{ \sigma^k(i) \mid k \in \mathbb{N} \right\}$$

(d) There is some $i \in 1\ldots n$ such that the domain of σ is the orbit of i under σ. That is the identity of

$$\mathrm{dom}(\sigma) \quad = \quad \left\{ \sigma^k(i) \mid k \in \mathbb{N} \right\}$$

(e) If $\ell := \mathrm{ord}(\sigma)$ denotes the order of σ, then there is some $i \in 1\ldots n$ such that the domain of σ is

$$\mathrm{dom}(\sigma) \quad = \quad \left\{ \sigma^k(i) \mid k \in 0\ldots(\ell-1) \right\}$$

And in this case the length ℓ of the cycle $\sigma = (i_1\ i_2\ \ldots\ i_\ell)$ is precisely the order of σ. That is the index ℓ in (a) equals the order of σ as an element of S_n

$$\mathrm{ord}(\sigma) \quad = \quad \ell \quad \text{in (a)}$$

(1.18) Proposition: (viz. 718)
Fix $n \in \mathbb{N}$ with $n \geq 1$ and consider the permutation group $(S_n, \circ)$. Remember that a *cycle* is special permutation $\sigma \in S_n$ that satisfies any of the equivalent properties in (1.17). Then, for permutation $\sigma \in S_n$ and any $i \in 1 \dots n$, we find the following statements

(i) We obtain an equivalence relation on $1 \dots n$ by letting $i \sim j$ if and only if there is some $k \in \mathbb{N}$ such that $j = \sigma^k(i)$. And the equivalence classes under this relation are precisely

$$[i] \;=\; \mathrm{cyc}(\sigma, i) \;=\; \Big\{ i, \sigma(i), \dots, \sigma^{k(i)}(i) \Big\}$$

where $k(i) := \ell(\sigma, i) - 1$. In particular $\mathrm{cyc}(\sigma, i)$ is σ-invariant: That is $\mathrm{cyc}(\sigma, i)$ remains fixed under σ, which formally reads as $\sigma(\mathrm{cyc}(\sigma, i)) = \mathrm{cyc}(\sigma, i)$. Let us now regard

$$\zeta_i \;:\; 1 \dots n \to 1 \dots n \; \begin{cases} \sigma(a) \text{ if } a \in \mathrm{cyc}(\sigma, i) \\ \quad a \text{ if } a \notin \mathrm{cyc}(\sigma, i) \end{cases}$$

That is ζ_i acts as σ on the cycle $\mathrm{cyc}(\sigma, i)$ but acts as the identity outside this cycle. Then ζ_i is precisely the cycle induced by σ on $i \in 1 \dots n$, formally again

$$\zeta_i \;=\; (i\ \sigma(i)\ \dots\ \sigma^{k(i)}(i))$$

And if $i(1), \dots, i(r)$ is a system of representative of $\mathrm{dom}(\sigma)$ under the relation $\sim$, that is $\mathrm{dom}(\sigma)$ is the disjoint union of the cycles $\mathrm{cyc}(\sigma, i(1))$ to $\mathrm{cyc}(\sigma, i(r))$, then σ can be written as the composition of the cycles $\zeta_{i(i)}$ to $\zeta_{i(r)}$ (in any order, as all the cycles are mutually commutative)

$$\mathrm{dom}(\sigma) \;=\; \bigcup_{j=1}^{r} \mathrm{cyc}(\sigma, i(j)) \quad\Longrightarrow\quad \sigma \;=\; \prod_{j=1}^{r} \zeta_{i(j)}$$

(ii) Let $\zeta_1, \dots, \zeta_k \in S_n$ and $\xi_1, \dots, \xi_t \in S_n$ be two sets of cycles, with pairwise disjoint domains, i.e.

$$\begin{aligned} i \neq j \in 1 \dots k \quad &\Longrightarrow \quad \mathrm{dom}(\zeta_i) \cap \mathrm{dom}(\zeta_j) = \emptyset \\ r \neq s \in 1 \dots t \quad &\Longrightarrow \quad \mathrm{dom}(\xi_r) \cap \mathrm{dom}(\xi_s) = \emptyset \end{aligned}$$

If now the compositions $\zeta_1 \dots \zeta_k = \xi_1 \dots \xi_t$ are equal, then we already get $k = t$ and there is some permutation $\alpha \in S_r$ such that for any $i \in 1 \dots k$ we get $\zeta_i = \xi_{\alpha(i)}$

$$\prod_{i=1}^{k} \zeta_i \;=\; \prod_{r=1}^{t} \xi_r \quad\Longrightarrow\quad \forall\, i \in 1 \dots k \;:\; \zeta_i = \xi_{\alpha(i)}$$

(iii) For any permutation $\sigma \in S_n$ with $\sigma \neq \mathbb{1}$ there is a uniquely determined **cyclic decomposition** $\{ \zeta_1, \dots, \zeta_r \}$ of σ. That is the $\zeta_1, \dots, \zeta_r \in S_n$ are cycles with pairwise disjoint domains (for any i, $j \in 1 \dots r$ that is $i \neq j \implies \mathrm{dom}(\zeta_i) \cap \mathrm{dom}(\zeta_j) = \emptyset$), such that σ can be written as a composition of these cycles. And this decomposition is unique, up to ordering the ζ_i

$$\sigma \;=\; \prod_{i=1}^{r} \zeta_i$$

(iv) Any permutation $\sigma \in S_n$ is a product of transpositions of two adjacent numbers. That is there are finitely many $i_0, \dots i_s \in \mathbb{N}$ such that for any $j \in 1 \dots r$ we get $|i_j - i_{j-1}| = 1$ and also

$$\sigma \;=\; \prod_{j=1}^{s} (i_{j-1} \;\; i_j)$$

(v) Two permutations ϱ and $\sigma \in S_n$ share the same cyclic structure if and only if they are conjugates of each other. Formally that is the equivalence of the following two statements

(a) If we decompose $\varrho = \zeta_1 \dots \zeta_k$ and $\sigma = \xi_1 \dots \xi_t$ into cycles, ζ_i and ξ_r respectively, with pairwise disjoint domains (as in (ii)), then we get $k = t$ and these cycles are of the same lengths. That is there is a permutation $\alpha \in S_k$ such that

$$\forall\, i \in 1 \dots k \;\; : \;\; \mathrm{ord}(\zeta_i) \;=\; \mathrm{ord}(\xi_{\alpha(i)})$$

(b) There is some permutation $\pi \in S_n$ such that $\sigma = \pi \varrho \pi^{-1}$.

(1.19) Example: Cyclic Decomposition:
Let us present a short example of a cyclic decomposition in $1 \dots 9$. To define or permutation $\sigma \in S_9$ we present a short table to fix σ

i	1	2	3	4	5	6	7	8	9
$\sigma(i)$	3	4	1	8	7	6	9	2	5

First of all it is clear that 6 is fixed under σ, hence it will not appear in our cyclic decomposition (it would yield a cycle of length 1, namely (6)). Now begin by 1 and extract its cycle. We see that $1 \mapsto 3 \mapsto 1$ so our first cycle is (1 3). The next number not dealt with is 2, which is cycled like $2 \mapsto 4 \mapsto 8 \mapsto 2$. So the second cycle is (2 4 8). As 3 and 4 occurred in the first and second cycles respectively, we continue with 5 which is moved like $5 \mapsto 7 \mapsto 9 \mapsto 5$. Thus the third cycle is (5 7 9). As 6 is fixed and $7 \dots 9$ have already been taken care of we have exhausted the whole domain of σ. Altogether we have seen that

$$\sigma \;=\; (1\,3)(2\,4\,8)(5\,7\,9)$$

Note that these cycles are uniquely determined even if there are several ways of putting them, e.g. $(2\ 4\ 8) = (4\ 8\ 2) = (8\ 2\ 4)$. Also it is possible to commute these cycles arbitrarily, without changing σ as they are mutually commutative. Finally we know, that any other permutation $\varrho \in S_9$ is conjugated to σ, if and only if it consists of 3 cycles of lengths 2,3,3 respectively.

(1.20) Definition:
Fix any $n \in \mathbb{N}$ with $n \geq 1$. If now σ is any permutation then we define the **signum** of this permutation to be the following number

$$\mathrm{sgn}(\sigma) \;:=\; \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

It will turn out that the signum is contained in $\mathrm{sgn}(\sigma) \in \mathbb{Z}^* = \{-1, +1\}$. A permutation σ with $\mathrm{sgn}(\sigma) = 1$ is said to be **even**, whereas a permutation with $\mathrm{sgn}(\sigma) = -1$ is said to be **odd**. The set of all even permutations will be denoted, by

$$A_n \;:=\; \{\, \sigma \in S_n \mid \mathrm{sgn}(\sigma) = 1 \,\}$$

(1.21) Remark:
The product, that has been used to define the signum of σ might be a little obfuscated at a first glance. But in fact the indexes simply run over the set $\Delta := \{\, (i,j) \in (1 \ldots n)^2 \mid i < j \,\}$. And as the multiplication in $\mathbb{Q}$ is commutative the ordering of this set Δ has no effect on the result of the product. In other words

$$\mathrm{sgn}(\sigma) \;=\; \prod_{i=1}^{n-1} \prod_{j=i+1}^{n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

As an example let us consider the case $\tau = (1\ 3) \in S_4$. Then the signum of the transposition τ can be computed, to be

$$\sigma(\tau) \;=\; \frac{2-3}{2-1} \cdot \frac{1-3}{3-1} \cdot \frac{4-3}{4-1} \cdot \frac{1-2}{3-2} \cdot \frac{4-2}{4-2} \cdot \frac{4-1}{4-3} \;=\; -1$$

(1.22) Proposition: (viz. 721)

(i) If $\sigma \in S_n$ is any permutation, then the signum of σ can be evaluated by counting the number of *inversions* of σ. That is the signum is given to be $\mathrm{sgn}(\sigma) = (-1)^{I(\sigma)}$ where

$$I(\sigma) \;:=\; \#\{\, (i,j) \in (1 \ldots n)^2 \mid i < j \text{ and } \sigma(i) > \sigma(j) \,\}$$

(ii) Let $\sigma \in S_n$ be a permutation and $\sigma = \zeta_1 \ldots \zeta_r$ be its decomposition into cycles with pairwise disjoint domains. Let $\ell(i) := \mathrm{ord}(\zeta_i)$ be the length of the i-th cycle. Then the order of σ is the least common multiple of the $\ell(i)$ and we can easily compute the signum of σ as well

$$\begin{aligned} \mathrm{ord}(\sigma) &= \mathrm{lcm}(\ell(1), \ldots, \ell(r)) \\ \mathrm{sgn}(\sigma) &= \prod_{i=1}^{r} (-1)^{\ell(i)-1} \end{aligned}$$

(iii) If $\sigma \in S_n$ is decomposed into the transpositions τ_i that is $\sigma = \tau_1 \tau_2 \ldots \tau_r$ where (for any $i \in 1 \ldots r$) τ_i is a cycle of length 2, then the signum of σ is just

$$\mathrm{sgn}(\sigma) \;=\; (-1)^r$$

(iv) For any $n \in \mathbb{N}$ with $n \geq 1$ the signum is a group homomorphism of the form $\mathrm{sgn} : S_n \to \mathbb{Z}^*$. That is for any $\varrho, \sigma \in S_n$ we get

$$\mathrm{sgn}(\varrho\sigma) \;=\; \mathrm{sgn}(\varrho) \cdot \mathrm{sgn}(\sigma)$$

(v) $(\diamondsuit)$ For any $n \in \mathbb{N}$ with $n \geq 2$ we find that $A_n \trianglelefteq_n S_n$ is a normal subgroup of S_n that has precisely half as many elements, as S_n does, that is

$$\#A_n \;=\; \frac{n!}{2}$$

1.3 Defining Rings

In the previous section we have introduced an atomic component - groups (and their generalizations monoids and groupoids). We have also introduced some notation, that we employ whenever we are dealing with these objects. We will glue two groupoids over the same set R together - that is we consider a set equipped with two binary relations $+$ and $\cdot$ that are compatible in some way (by distributivity). Note that we again write $a+b$ instead of $+(a,b)$ and likewise $a \cdot b$ (or shorthand ab only) for $\cdot(a,b)$. These objects will be called rings and we will dedicate the entire first part of this book to rings and the structure they may have.

(1.23) Definition:
Let $R \neq \emptyset$ be any non-empty set and consider two binary operations $+$ called **addition** and $\cdot$ called **multiplication** on R. And the ordered tripel $(R,+,\cdot)$ is said to be **ringoid** iff it satisfies both of the following properties (A) and (D), where

$$\begin{aligned} + \;&:\; R \times R \to R \;&:\; (a,b) \mapsto a+b \\ \cdot \;&:\; R \times R \to R \;&:\; (a,b) \mapsto a \cdot b \end{aligned}$$

(A) $(R,+)$ is a commutative group, that is the addition is *associative* and *commutative*, admits a neutral element (called *zero-element* and denoted by 0) and every element of R has an additive inverse. Formally that is

$$\begin{aligned} \forall\, a,b,c \in R \;&:\; a+(b+c) \;=\; (a+b)+c \\ \forall\, a,b \in R \;&:\; a+b \;=\; b+a \\ \exists\, 0 \in R\; \forall\, a \in R \;&:\; a+0 \;=\; a \\ \forall\, a \in R\; \exists\, n \in R \;&:\; a+n \;=\; 0 \end{aligned}$$

Note that the **zero-element** 0 thereby is already uniquely determined and hence the fourth property makes sense. Further, if we are given $a \in R$, then the element $n \in R$ with $a+n=0$ is uniquely determined, and we call it the **negative** of a, denoted by $-a := n$.

(D) The addition and multiplication on R respect the following *distributivity laws*, i.e. $\forall\, a,b,c \in R$ we have the properies

$$\begin{aligned} a \cdot (b+c) \;&=\; (a \cdot b)+(a \cdot c) \\ (a+b) \cdot c \;&=\; (a \cdot c)+(b \cdot c) \end{aligned}$$

As is the structure of a ringoid is very general and hence hard to pin down. We will consider rings and commutative rings only, where the multiplication also is a (commutative) monoid. The prominent examples of matrix algebras and the integers are of this kind and we will see, that in this case we can tell a lot about the structure of such rings.

(1.24) Definition:
In the following let $(R,+,\cdot)$ be a ringoid, then we consider a couple ofvadditional properties (S), (R) and (C), that R may or may not have and introduce names to these

(C) The multiplication $\cdot$ on R is *commutative*, that is we have the property

$$\forall\, a,b,c \in R \;:\; a\cdot b \;=\; b\cdot a$$

(S) The multiplication $\cdot$ on R is *associative*, that is we have the property

$$\forall\, a,b,c \in R \;:\; a\cdot(b\cdot c) \;=\; (a\cdot b)\cdot c$$

(R) The multiplication $\cdot$ on R admits a *neutral element* 1, that is we have property

$$\exists 1 \in R\ \forall\, a \in R \;:\; 1\cdot a \;=\; a \;=\; a\cdot 1$$

Note that the neutral element 1 of the multiplication of R already is uniquely determined and will be called the **unit-element** of R.

(F) Let us assume that R satisfies properties (S) and (R), then we define property (F): Every non-zero element R has an *inverse element*, that is

$$\forall\, 0 \neq a \in R\ \exists\, i \in R \;:\; a\cdot i \;=\; 1 \;= i\cdot a$$

Note that 1 is given by (R) and due to (S) the element $i \in R$ is uniquely determined by a. We call i the **inverse** of a, denoted by $a^{-1} := i$.

Using these properties we define the following notions: Let $(R,+,\cdot)$ be a ringoid, then $(R,+,\cdot)$ is even said to be **commutative** resp. called a **semi-ring**, **ring**, **skew-field** of even **field**, iff

commutative	$:\Longleftrightarrow$	(C)
semi-ring	$:\Longleftrightarrow$	(S)
ring	$:\Longleftrightarrow$	(S) and (R)
commutative ring	$:\Longleftrightarrow$	(S), (R) and (C)
skew-field	$:\Longleftrightarrow$	(S), (R), (F) and $0 \neq 1$
field	$:\Longleftrightarrow$	(S), (R), (C), (F) and $0 \neq 1$

Nota in the mathematical literature the word *ring* may have many different meanings, depending of what topic a given text pursues. While some authors do not assume rings to have a unit (or even not be associative) others assume them to always be commutative. Hence it also is customary to speak of a *non-unital ring* in case of a semi-ring and of a *unital ring* in case of a ring.

(1.25) Remark:
Let $(R,+,\cdot)$ be a ringoid, then we simplify our notation somewhat by introducing the following conventions

- The zero-element of any ringoid R is denoted by 0. If we deal with several ringoids simultaneously then we will write 0_R to emphasize, which ringoid the zero-element belongs to.
- Analogously the unit element of any ring R is denoted by 1 and by 1_R if we wish to stress the ring R. For some specific rings we will use a different symbol than 1, e.g. $\mathbf{1}$ or $\mathbb{1}$.
- In order to save some parentheses we agree that the multiplication $\cdot$ is of higher priority than the addition $+$, e.g. from now on $ab+c$ shall abbreviate $(a\cdot b)+c$.
- The addition of the additive inverse is sometimes used just like a binary operation itself, i.e. $a-b$ stands shortly for $a+(-b)$.
- We have introduced the multiplicative inverse a^{-1} of a and we use the convention that the inversion is of higher priority, than the multiplication itself, i.e. ab^{-1} stands shortly for $a\cdot(b^{-1})$.
- If $a_1,\ldots,a_n\in R$ are finitely many elements of R, then we denote the **sum** and **product** of these to be the following element of R again

$$\begin{aligned}\sum_{i=1}^{n} a_i &:= \Big((a_1+a_2)+\ldots\Big)+a_n\\ \prod_{i=1}^{n} a_i &:= \Big((a_1\cdot a_2)\cdot\ldots\Big)\cdot a_n\end{aligned}$$

- For some integer $k\in\mathbb{Z}$ we now introduce the following abbreviations

$$ka := \begin{cases} \sum_{i=1}^{k} a \text{ for } k>0\\ 0 \text{ for } k=0\\ \sum_{i=1}^{-k}(-a) \text{ for } k<0\end{cases}$$

$$a^k := \begin{cases} \prod_{i=1}^{k} a \text{ for } k>0\\ 1 \text{ for } k=0\\ \prod_{i=1}^{-k}(a^{-1}) \text{ for } k<0\end{cases}$$

 For the definition of a^k we, of course, required R to be a ring in the case $k=0$ and even that a is *invertible* (refer to the next section for this notion) in the case $k<0$.

(1.26) Remark:

- Consider any ringoid $(R, +, \cdot)$, then the addition $+$ on R is associative by definition. Hence the result of the sum $a_1 + \cdots + a_n \in R$ does not depend on the way we applied parentheses to it (cf. (1.2)). Therefore we may equally well omit the bracketing in the summation, writing

$$a_1 + \cdots + a_n \;:=\; \sum_{i=1}^{n} a_i$$

 The same is true for the multiplication $\cdot$ in a semi-ring $(R, +, \cdot)$. So by the same reasoning we omit the brackets in products, writing

$$a_1 \ldots a_n \;:=\; \prod_{i=1}^{n} a_i$$

- By definition the addition $+$ of a ringoid $(R, +, \cdot)$ also is commutative. Thus the sum $a_1 + \cdots + a_n \in R$ does not even depend on the ordering of the a_i (refer to (1.2) again). Now take any finite set Ω and regard a mapping $a : \Omega \to R$. Then we may even define the sum over the unordered set Ω. To do this fix any bijection of the form $\sigma : 1 \ldots n \longleftrightarrow \Omega$ (in particular $n := \#\Omega$). Then we may define

$$\sum_{i \in \Omega} a(i) \;:=\; \begin{cases} 0 \text{ if } \Omega = \emptyset \\ \sum_{i=1}^{n} a(\sigma(i)) \text{ if } \Omega \neq \emptyset \end{cases}$$

 The same is true for the multiplication $\cdot$ in a commutative semi-ring $(R, +, \cdot)$. So given $a : \Omega \to R$ and σ as above we define (note that the case $\Omega = \emptyset$ even requires R to be a commutative ring)

$$\prod_{i \in \Omega} a(i) \;:=\; \begin{cases} 1 \text{ if } \Omega = \emptyset \\ \prod_{i=1}^{n} a(\sigma(i)) \text{ if } \Omega \neq \emptyset \end{cases}$$

- If I is infinite but the set $\Omega := \{\, i \in I \mid a(i) \neq 0 \,\}$ is finite still we write an infinte sum over all $i \in I$, that actually is defined by a finite sum

$$\sum_{i \in I} a(i) \;:=\; \sum_{i \in \Omega} a(i)$$

 If R is a commutative ring and analogously $\Omega := \{\, i \in I \mid a(i) \neq 1 \,\}$ is finite then the same is true for the infinite product

$$\prod_{i \in I} a(i) \;:=\; \prod_{i \in \Omega} a(i)$$

1.4 Examples

(1.27) Example:

- The most well-known example of a commutative ring are the integers $(\mathbb{Z}, +, \cdot)$. And they are a most beautiful ring indeed - e.g. $\mathbb{Z}$ does not contain zero-divisors (that is $ab = 0$ implies $a = 0$ or $b = 0$). And we only wish to remark here that $\mathbb{Z}$ is an UFD (that is any $a \in \mathbb{Z}$ admits a unique primary decomposition) - this will be the formulated and proved as the fundamental theorem of arithmetic.
- Now regard the set $2\mathbb{Z} := \{ 2a \mid a \in \mathbb{Z} \}$ of even integers. It is easy to see, that the sum and product of even numbers again is even. Hence $(2\mathbb{Z}, +, \cdot)$ is a (commutative) semi-ring under the operations inherited from $\mathbb{Z}$. Yet it does not contain a unit element 1 and hence does not qualify to be a ring.
- Next we will regard a somewhat strange ring, the so called *zero-ring* Z. As a set it is defined to be $Z := \{0\}$ (with $0 \in \mathbb{Z}$ if you wish). As it solely contains one point 0 it is clear how the binary operations have to be defined $0 + 0 := 0$ and $0 \cdot 0 := 0$. It is esy to check that $(Z, +, \cdot)$ thereby becomes a commutative ring in which $1 = 0$. We will soon see that Z even is the only ring in which $1 = 0$ holds true. In this sense this ring is a bit pathological.
- Now consider an arbitrary (commutative) ring $(R, +, \cdot)$ and a non-empty set $I \neq \emptyset$. Then the set R^I of functions from I to R can be turned into another (commutative) ring $(R^I, +, \cdot)$ under the *point-wise* operations of functions

$$R^I := \{ f \mid f : I \to R \}$$

$$f + g : I \to R : i \mapsto f(i) + g(i)$$

$$f \cdot g : I \to R : i \mapsto f(i) \cdot g(i)$$

- Let X be any set and denote its *power set* by $\mathcal{P}(X) := \{ A \mid A \subseteq X \}$. And for any subsets A, $B \subseteq X$ we define the *symmetric difference* $A \,\Delta\, B := (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A) \subseteq X$. Thereby $(\mathcal{P}(X), \Delta, \cap)$ becomes a commutative ring with zero-element $\emptyset$ and unit element X. And if $A \subseteq X$ is any subset, then the additive inverse of A is just $-A = A$ again.
- The next ring we study are the rational numbers $(\mathbb{Q}, +, \cdot)$. It is well-known that $\mathbb{Q}$ even is a field - if $a/b \neq 0$ then $a \neq 0$ and hence $(a/b)^{-1} = (b/a)$ is invertible. We will even present a construction of gaining $\mathbb{Q}$ from $\mathbb{Z}$ in example (1.31), in this section.
- Most of the previous examples have been quite large (considering the number of elements involved). We would now like to present an example of a finite field consisting of precisely four elements $F = \{ 0, 1, a, b \}$. As F is finite, we may give the addition and multiplication in tables

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

(1.28) Example:
Having introduced $\mathbb{Z}$, $\mathbb{Q}$ and the reals $\mathbb{R}$ we would like to turn our attention to another important case - the *residue rings* of $\mathbb{Z}$. First note, that the integers $\mathbb{Z}$ allow a division with remainder (cf. to section 2.7). That is if we fix $2 \leq n \in \mathbb{N}$ then for any $a \in \mathbb{Z}$ then there are uniquely determined numbers $q \in \mathbb{Z}$ and $r \in 0 \ldots (n-1)$ such that

$$a \;=\; qn + r$$

Thereby r is called the *remainder* of a in the integer division of a times n. Formally one denotes (which is common in programming languages) the following operations

$$\begin{aligned} a \text{ div } n &:= q \\ a \text{ mod } n &:= r \end{aligned}$$

And by virtue of this operation "mod" we may now define the residue ring $(\mathbb{Z}_n, +, \cdot)$ of $\mathbb{Z}$ modulo n. First let $\mathbb{Z}_n := \{\, 0, 1, \ldots, n-1 \,\}$ as a set. And if a, $b \in \mathbb{Z}_n$, then we define the operations

$$\begin{aligned} a + b &:= (a + b) \text{ mod } n \\ a \cdot b &:= (a \cdot b) \text{ mod } n \end{aligned}$$

Thereby $(\mathbb{Z}_n, +, \cdot)$ will in fact be a commutative ring. And $\mathbb{Z}_n$ will be a field if and only if n is a prime number. We will soon give a more natural construction of $\mathbb{Z}_n$ as the quotient $\mathbb{Z}/n\mathbb{Z}$, as this will be far better suited to derive the properties of this ring.

(1.29) Example: (viz. 724)
Any semi-ring $(S, +, \cdot)$ can be embedded into a ring. In this sense the theory sub-semi-rings of rings encompassed the theory of semi-rings. The construction can be done in the following way: Take R to be the set $R := \mathbb{Z} \times S$ and equip R with the following two operations for any a, $b \in \mathbb{Z}$ and x, $y \in S$

$$\begin{aligned} (a, x) + (b, y) &:= (a + b, x + y) \\ (a, x) \cdot (b, y) &:= (ab, ay + bx + xy) \end{aligned}$$

Then $(R, +, \cdot)$ becomes a ring with zero-element $0_R = (0, 0_S)$ and unit $1_R = (1, 0_S)$. Note that R is commutative, if and only if S is commutative. And we can interpret S as a sub-ring of R under the canonical embedding [that is injective and satisfies $\iota(x + y) = x + y$ and $\iota(xy) = xy$]

$$\iota : S \hookrightarrow R : x \mapsto (0, x)$$

(1.30) Example: $(\diamondsuit)$

Let $(R,+,\cdot)$ be an arbitrary ring, we will later employ the **opposite ring** $(R,+,\cdot)^{\mathrm{op}}$ of R. This is defined to be R as a set, under the same addition $+$ but with a multiplication that reverses the order of elements. Formally

$$(R,+,\cdot)^{\mathrm{op}} := (R,+,\circ) \quad \text{where} \quad a \circ b := b \cdot a$$

Note that thereby $(R,+,\cdot)^{\mathrm{op}}$ is a ring again with the same properties as $(R,+,\cdot)$ before. And if $(R,+,\cdot)$ has been commutative, then the opposite ring of R is just R itself, i.e. $(R,+,\cdot)^{\mathrm{op}} = (R,+,\cdot)$.

(1.31) Example:

Let $(R,+,\cdot)$ be an *integral domain*, that is $R \neq 0$ is a non-zero commutative ring such that for any two elements a, $b \in R$ we have: Whenever $ab = 0$ then we necessarily have $a = 0$ or $b = 0$. In this case we take to the set $X := R \times (R \setminus \{0\})$ and obtain an equivalence relation $\sim$ on X by letting

$$(a,u) \sim (b,v) \quad :\Longleftrightarrow \quad av = bu$$

for any (a,u) and $(b,v) \in X$. If now $(a,u) \in X$ then we denote its equivalence class by a/u, and let us denote the quotient set of X modulo $\sim$ by Q. Formally that is

$$\begin{aligned} \frac{a}{u} &:= \{\, (b,v) \in X \mid av = bu \,\} \\ Q &:= \left\{ \frac{a}{u} \;\middle|\; a,b \in R,\ b \neq 0 \right\} \end{aligned}$$

Thereby Q becomes a commutative ring (with zero-element $0/1$ and unit element $1/1$) under the following (well-defined) addition and multiplication

$$\begin{aligned} \frac{a}{u} + \frac{a}{u} &:= \frac{av + bu}{uv} \\ \frac{a}{u} \cdot \frac{a}{u} &:= \frac{ab}{uv} \end{aligned}$$

In fact $(Q,+,\cdot)$ even is a field, called the *quotient field* of R. This is due to the fact that the inverse of $a/u \neq 0/1$ is given to be $(a/u)^{-1} = u/a$. This construction will be vastly generalized in section 2.10. Note that this is precisely the way to obtain the rationals $\mathbb{Q} := Q$ by starting with $R = \mathbb{Z}$.

(1.32) Example:

Consider an arbitrary ring $(R,+,\cdot)$ and $1 \leq n \in \mathbb{N}$, then an $(n \times n)$-*matrix* over R is a mapping of the form $A : (1 \ldots n) \times (1 \ldots n) \to R$. And we denote the set of all such maps by $\mathrm{mat}_n(R)$ that is $\mathrm{mat}_n(R) := \{\, A \mid A : (1 \ldots n) \times (1 \ldots n) \to R \,\}$. Usually a matrix is written as an array of the following form (where $a_{i,j} := A(i,j)$)

$$A \;=\; \left(a_{i,j}\right) \;=\; \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix}$$

And using this notation we may turn $\mathrm{mat}_n(R)$ into a (non-commutative even if R is commutative) ring by defining the addition and multiplication

$$\Big(a_{i,j}\Big) + \Big(b_{i,j}\Big) \;:=\; \Big(a_{i,j} + b_{i,j}\Big)$$

$$\Big(a_{i,j}\Big) \cdot \Big(b_{i,j}\Big) \;:=\; \left(\sum_{s=1}^{n} a_{i,s}\, b_{s,j}\right)$$

It is immediately clear from the construction, that the zero-element, resp. the unit-element are given by the *zero-matrix* and *unit-matrix* respectively

$$0 \;=\; \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$$

$$1 \;=\; \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

(1.33) Example:
The following construction is of astounding importance. We will generalize it to several variablen, in (7.21). In fact we will dedicate the entire chapter 7 to it. But we will already use the one-variable case before, so make sure you understand the following construction: Let $(R, +, \cdot)$ be any commutative ring, we first define the (commutative) ring of *formal power series* over R, to be the set of functions from $\mathbb{N}$ to R. That is, as a set set, we define $R[\![t]\!]$ to be

$$R[\![t]\!] \;:=\; \{\, f \mid f : \mathbb{N} \to R \,\}$$

For any $f \in R[\![t]\!]$ we will write $f[k]$ instead of $f(k)$, that is $f : k \mapsto f[k]$. Further we denote f in the following form (note that this is purely notational and *not* a true sum)

$$\sum_{k=0}^{\infty} f[k]\, t^k \;:=\; f$$

And thereby we may define the sum and product of two formal power series $f, g \in R[\![t]\!]$, by point-wise summation $f + g : k \mapsto f[k] + g[k]$ and the involution $f \cdot g : k \mapsto f[0]g[k] + f[1]g[k-1] + \cdots + f[k]g[0]$. In terms of the above notation that is

$$f + g \;:=\; \sum_{k=0}^{\infty} \Big(f[k] + g[k]\Big) t^k$$

$$f \cdot g \;:=\; \sum_{k=0}^{\infty} \left(\sum_{i+j=k} f[i]g[j]\right) t^k$$

An elementary computation (cf. section 7.2) shows that $(R[\![t]\!], +, \cdot)$ truly becomes a commutative ring. The zero-element of this ring is given by $0 : k \mapsto 0$ and the unit element is $\mathbf{1} = t^0 : k \mapsto \delta(k,0)$. The element $t : k \mapsto \delta(k,1)$ plays another central role. An easy computation shows that for any $n \in \mathbb{N}$ we get $t^n : k \mapsto \delta(k,n)$. If now $0 \neq f \in R[\![t]\!]$ is a non-zero formal power series we define the *degree* of f

$$\deg(f) \;:=\; \sup\{\, k \in \mathbb{N} \mid f[k] \neq 0 \,\} \;\in\; \mathbb{N} \cup \{\infty\}$$

That is $\deg(f) < \infty$ just states that the set $\{\, k \in \mathbb{N} \mid f[k] \neq 0 \,\}$ is a finite subset of $\mathbb{N}$. And thereby we define the *polynomial ring* over R to be set of power series of finite degree

$$R[t] \;:=\; \{\, f \in R[\![t]\!] \mid \deg(f) < \infty \,\}$$

By definition $R[t] \subseteq R[\![t]\!]$ is a subset, but one easily verifies, that $R[t]$ even is another commutative ring under the addition and multiplication inherited from $R[\![t]\!]$. Further note that every polynomial $f \in R[t]$ now truly is a finite sum of the form

$$f \;=\; \sum_{k=0}^{\infty} f[k]\, t^k$$

If $f \in R[t]$ the highest non-zero coefficient of f will be called the **leading coefficient** of f, denoted by $\mathrm{lc}(f)$. And f is said to be a **monic** polynomial, iff $f \neq 0$ and its leading coefficient is $1 \in R$

$$\mathrm{lc}(f) \;:=\; \begin{cases} f[\deg(f)] \text{ if } f \neq 0 \\ 0 \text{ if } f = 0 \end{cases} \;\in\; R$$

(1.34) Remark:
The field of real numbers is a very peculiar one. You most probably know it from high school already, although it actually is not so simple, at all. If it wasn't used so frequently, we would well postpone it until much later. Stick to the intuition, that the real numbers x is expressions of the form $x = a + 0.d_1d_2d_3\ldots$, where $a \in \mathbb{Z}$ is an integer and the d_i are digits $d_i \in 0\ldots9$. Then the value of x is

$$x \;=\; a + \sum_{i=1}^{\infty} d_i\, 10^{-i}$$

Actually this rather is a way of addressing x, as a point on a line, than a value. But we will set out onto a lengthy journey to give a meaning to this. The best way to deal with the field $\mathbb{R}$ of reals is understanding the following list of properties, that uniquely determine $\mathbb{R}$ (up to isomorphy). First of all $(\mathbb{R}, +, \cdot)$ is a field of course. But there also is a *total order* $\leq$ on $\mathbb{R}$ - in the sense of (0.17) - that also is *positive* - in the sense of (1.87). That is $\leq$ is a total order, such that $0 \leq 1$ for any $x, y \in \mathbb{R}$ we have

(1) $x \leq y \iff 0 \leq y - x$

(2) $0 \leq x, y \implies 0 \leq x + y$

(3) $0 \leq x, y \implies 0 \leq xy$

These properties have several consequences, in themselves, as we will see in section (1.8). But $\mathbb{R}$ also has the following *supremum property*: Recall, that for a subset $A \subseteq \mathbb{R}$ and $b \in \mathbb{R}$ we defined $A \leq b$ by $\forall\, a \in A : a \leq b$. Such a b is said to be an *upper bound* of A. Now

(4) If A is a non-empty set of real numbers, that A has an upper bound, there A already has a minimal upper bound s. Formally put this property reads as

$$\begin{aligned} \forall\, A \subseteq \mathbb{R} \;\; &: \;\; A \neq \emptyset \text{ and } \exists\, b \in \mathbb{R} : A \leq b \\ \exists\, s \in \mathbb{R} \;\; &: \;\; A \leq s \text{ and } \forall\, b \in \mathbb{R} : A \leq b \implies s \leq b \end{aligned}$$

This minimal upper bound s then is uniquely determined and will be denoted, by $s = \sup(A)$. Prob suppose that both, r and s have this property, then in particular $A \leq r$ and $A \leq s$. But as both r and s are minimal with this property, we get $s \leq r$ and $r \leq s$ such that $r = s$.

($\diamondsuit$) We recommend, that the reader takes these properties for granted. For the more experienced reader we want to continue by giving an algebraic construction of $\mathbb{R}$, of which it can be shown, that is satisfies these properties: Let us denote the sets of Cauchy-sequences and zero-sequences over the rational numbers $\mathbb{Q}$ respectively

$$\mathcal{C} \;:=\; \left\{ (q_n) \subseteq \mathbb{Q} \;\middle|\; \begin{array}{l} \forall\, k \in \mathbb{N}\; \exists\, n(k) \in \mathbb{N} \\ \forall\, m,n \geq n(k) \;:\; |q_n - q_m| < 1/k \end{array} \right\}$$

$$\mathfrak{z} \;:=\; \left\{ (q_n) \subseteq \mathbb{Q} \;\middle|\; \begin{array}{l} \forall\, k \in \mathbb{N}\; \exists\, n(k) \in \mathbb{N} \\ \forall\, n \geq n(k) \;:\; |q_n| < 1/k \end{array} \right\}$$

Then $\mathcal{C}$ becomes a commutative ring under the point-wise operations $(p_n) + (q_n) := (p_n + q_n)$ and $(p_n)(q_n) := (p_n q_n)$ of maps. And $\mathfrak{z} \trianglelefteq_{\mathrm{i}} \mathcal{C}$ is a maximal ideal of $\mathcal{C}$ (cf. to section 2.1). Now the reals can be introduced as the quotient (cf. to section 1.6) of $\mathcal{C}$ modulo $\mathfrak{z}$

$$\mathbb{R} \;:=\; \mathcal{C} \Big/ \mathfrak{z}$$

As $\mathfrak{z}$ has been maximal $\mathbb{R}$ becomes a field (see 2.5). Thereby $\mathbb{Q}$ can be embedded into $\mathbb{R}$, by virtue of $\mathbb{Q} \hookrightarrow \mathbb{R} : q \mapsto (q)$. And we obtain a positive order on $\mathbb{R}$ by letting $(p_n) + \mathfrak{z} \leq (q_n) + \mathfrak{z}$ iff $\exists\, m \in \mathbb{N}\; \forall\, n \geq m : p_n \leq q_n$. Note that this *completion* of $\mathbb{Q}$ (that is Cauchy-sequences modulo zero-sequences) can be generalized to arbitrary metric spaces (see section 3.14). Its effect is that the resulting space becomes *complete* (that is Cauchy sequences are already convergent). In our case this also guarantees the supremum-property. And with this construction we are finally able to give meaning to the representation of x as a decimal number. The x at the beginning of this example is $x = (q_n) + \mathfrak{z}$, where

$$q_n \;=\; a + \sum_{i=1}^{n} d_i\, 10^{-i} \;\in\; \mathbb{Q}$$

(1.35) Example:
The complex numbers $(\mathbb{C}, +, \cdot)$ also form a field (that even has a lot of properties that make it better-behaved than the reals). We want to present three (isomorphic) ways of introducing $\mathbb{C}$ now:

(1) First of all define $\mathbb{C} := \mathbb{R}^2$ to be the real plane. For any two complex numbers $z = (a,b)$ and $w = (c,d)$ we define the operations

$$\begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} c \\ d \end{pmatrix} \;:=\; \begin{pmatrix} a+c \\ b+d \end{pmatrix}$$

$$\begin{pmatrix} a \\ b \end{pmatrix} \cdot \begin{pmatrix} c \\ d \end{pmatrix} \;:=\; \begin{pmatrix} ad-bc \\ ac+bd \end{pmatrix}$$

The advantage of this construction is, that it is purely elementary. The disadvantage is that one has to check that $(\mathbb{C},+,\cdot)$ truly becomes a field under these operations (which we leave as an exercise). We only present the inverse of $(0,0) \neq z = (a,b) \in \mathbb{C}$. Define the *complex conjugate* of z to be $\overline{z} := (a,-b)$ and let $\nu(z) := z\overline{z} = a^2+b^2 \in \mathbb{R}$, then $z^{-1} = (a\nu(z)^{-1}, -b\nu(z)^{-1})$. Let us now denote $1 = (1,0)$ and $i = (0,1) \in \mathbb{C}$, then it is clear, that 1 is the unit element of $\mathbb{C}$ and that $i^2 = -1$. Further any $z = (a,b) \in \mathbb{C}$ can be written uniquely, as $z = a1 + bi$. It is customary to write $z = a + ib$ for this however.

(2) $(\diamondsuit)$ The next construction will imitate the one in (1) - yet it realizes (a,b) as a real (2×2)-matrix. This has the advantage, that addition and multiplication are well-known for matrices

$$\mathbb{C} \;:=\; \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \;\middle|\; a,b \in \mathbb{R} \right\}$$

It is straightforward to see that $\mathbb{C}$ thereby becomes a field under the addition and multiplication of matrices, that coincides with the one introduced in (1) (check this, it's neat). Note that thereby the determinant plays the role of $\nu(z) = \det(z)$ and the transposition of matrices is the complex conjugation $\overline{z} = z^*$.

(3) $(\diamondsuit)$ The third method implements the idea that i is introduced in such a way as to $i^2 = -1$. We simply force a solution of $t^2+1 = 0$ into $\mathbb{C}$

$$\mathbb{C} \;:=\; \mathbb{R}[t] \Big/ (t^2+1)\mathbb{R}[t]$$

Comparing this construction with the one in (1) we have to identify (a,b) with $a + bt + (t^2+1)\mathbb{R}[t]$. In particular $i = t + (t^2+1)\mathbb{R}[t]$. Then it again is easy to see, that addition and multiplication coincide under this identification. The advantage of this construction is that it focusses on the idea of finding a solution to $t^2+1 = 0$ (namely i), that $\mathbb{C}$ immediately is a field (as t^2+1 is prime, $\mathbb{R}[t]$ is a PID and hence $(t^2+1)\mathbb{R}[t]$ is maximal). The disadvantage is that it already requires the algebraic machinery, which remains to be introduced here. We will generalize this in (7.76).

(1.36) Example: $(\diamondsuit)$

Let us now present an example of an infinite commutative group, that is a subgroup of the multiplicative group $\mathbb{C}^*$ of the complex numbers. Fix any prime number $2 \leq p \in \mathbb{Z}$, then we let

$$\Gamma_p \;:=\; \left\{ \exp\left(\frac{2m\pi i}{p^n}\right) \;\middle|\; m,\, n \in \mathbb{N} \right\}$$

Thereby the operation of Γ_p is just the multiplication of complex numbers (as Γ_p is a subgroup of $\mathbb{C}^*$). For the inverse of an element in Γ_p choose some $k \in \mathbb{N}$ such that $kp^n > m$, then

$$\exp\left(\frac{2m\pi i}{p^n}\right)^{-1} \;=\; \exp\left(\frac{2(kp^n-m)\pi i}{p^n}\right)$$

(1.37) Example: $(\diamondsuit)$

Now fix any square-free $0 \neq d \in \mathbb{Z}$ (d being *sqare-free* means that there is no prime number $p \in \mathbb{Z}$ such that p^2 divides d). Then we define the following subset of the real resp. complex numbers

$$\mathbb{Z}[\sqrt{d}] \;:=\; \left\{ a + b\sqrt{d} \mid a, b \in \mathbb{Z} \right\}$$

Note that $\mathbb{Z}[\sqrt{d}]$ is contained in the reals if and only if $0 < d$, and in the case of $d < 0$ we have $\sqrt{d} = i\sqrt{-d} \in \mathbb{C}$. In any case $\mathbb{Z}[\sqrt{d}]$ becomes a commutative ring under the addition and multiplication inherited from $\mathbb{C}$

$$\begin{aligned} (a + b\sqrt{d}) + (e + f\sqrt{d}) &= (a + e) + (b + f)\sqrt{d} \\ (a + b\sqrt{d}) \cdot (e + f\sqrt{d}) &= (ae + dbf) + (af + be)\sqrt{d} \end{aligned}$$

It will be most interesting to see how the algebraic properties of these rings vary with d. E.g. for $d \in \{ -2, -1, 2, 3 \}$ the ring $\mathbb{Z}[\sqrt{d}]$ will be an Euclidean domain under $v(a + b\sqrt{d}) := |a^2 - db^2|$ as an Euclidean function. Yet $\mathbb{Z}[\sqrt{d}]$ will not even be an UFD for $d \leq -3$.

(1.38) Example:

We have just introduced the complex numbers as a two-dimensional space $\mathbb{R}$ over the reals. The next (and last sensibly possible, cf. to the Theorem of Frobenius) step in the hierarchy leads us to the *quaternions* $\mathbb{H}$. These are defined to be a four-dimensional, space $\mathbb{H} := \mathbb{R}^4$ over the reals. And analogous to the above we specifically denote four elements

$$\begin{aligned} 1 &:= (1, 0, 0, 0) \\ i &:= (0, 1, 0, 0) \\ j &:= (0, 0, 1, 0) \\ k &:= (0, 0, 0, 1) \end{aligned}$$

That is any element $z = (a, b, c, d) \in \mathbb{H}$ can be written uniquely, in the form $z = a + ib + jc + kd$. The addition of elements of $\mathbb{H}$ is point-wise and the multiplication is then given by linear expansion of the following multiplication table for these basis elements

	1	i	j	k
1	1	i	j	k
i	i	-1	k	-j
j	j	-k	-1	i
k	k	j	-i	-1

For $z = a + ib + jc + kd$ and $w = p + iq + jr + ks \in \mathbb{H}$ these operations explicitly read as

$$\begin{aligned} z + w &= (a + p) + i(b + q) + j(c + r) + k(d + s) \\ zw &= (ap - bq - cr - ds) + i(aq + bp + cs - dr) \\ &\quad + j(ar - bs + cp + dq) + k(as + br - cq + dp) \end{aligned}$$

As with the complex numbers we define a *conjugation* on $\mathbb{H}$ by letting $\overline{z} := a - ib - jc - kd$. We also define $\nu(z) = z\overline{z} = a^2 + b^2 + c^2 + d^2 \in \mathbb{R}$ and the *real* and $\mathrm{re}(z) := a \in \mathbb{R}$ and *imaginary part* $\mathrm{im}(z) := (b, c, d) \in \mathbb{R}^3$ of z. Then the inverse of any $z \neq 0$ can be computed as

$$z^{-1} \;=\; \nu(z)^{-1}\overline{z} \;=\; \Big(a\nu(z)^{-1}, -b\nu(z)^{-1}, -c\nu(z)^{-1}, -d\nu(z)^{-1}\Big)$$

Yet $\mathbb{H}$ clearly is not commutative, as $ij = k = -ji$. Thus the quaternions form a skew-field, but not a field. Using the complex numbers $\mathbb{C}$ we may also realize the quaternions as (2×2)-matrices over $\mathbb{C}$. Given $a + ib + jc + kd \in \mathbb{H}$ we pick up the complex numbers $z = a + ib$ and $w = c + id \in \mathbb{C}$ and identify $a + ib + jc + kd$ with a (2×2)-matrix of the following form

$$\mathbb{H} \;\cong_{\mathsf{r}}\; \left\{ \left(\begin{array}{cc} z & w \\ -\overline{w} & \overline{z} \end{array} \right) \;\middle|\; z, w \in \mathbb{C} \right\}$$

$(\diamondsuit)$ Let us analyse the multiplication a little further: For $a \in \mathbb{R}$ and $u = (b, c, d) \in \mathbb{R}^3$ let us denote $(a, u) := a + ib + jc + kd \in \mathbb{H}$. Likewise we get $w = (p, v)$ for $v = (q, r, s)$. Then the conjugation of z is just $\overline{z} = (a, -u)$ and the multiplication of quaternions can be expressed using the scalar and the wedge product of $\mathbb{R}^3$, which we will introduce in (4.125)

$$(a, u) \cdot (p, v) \;:=\; \Big(ap - \langle u, v\rangle,\; av + pu + u \wedge v\Big)$$

(1.39) Example: $(\diamondsuit)$
The next example is primarily concerned with ideals, not with rings, and should hence be postponed until you want to study an example of these. Now fix any (commutative) base ring $(R, +, \cdot)$ and a non-empty index set $I \neq \emptyset$. We have already introduced the ring $S := R^I = \mathcal{F}(I, R)$ of functions from I to R under the point-wise operations. For any subset $A \subseteq I$ we now obtain an ideal of S by letting

$$\mathfrak{v}(A) \;:=\; \{\, f \in S \mid \forall\, a \in A : f(a) = 0 \,\}$$

This is called the *vanishing ideal* if A. And for any two subsets $A, B \subseteq I$ it is easy to prove the identities

$$\mathfrak{v}(A)\,\mathfrak{v}(B) \;=\; \mathfrak{v}(A) \cap \mathfrak{v}(B) \;=\; \mathfrak{v}(A \cup B)$$

$$\mathfrak{v}(A) + \mathfrak{v}(B) \;=\; \mathfrak{v}(A \cap B)$$

Clearly (if I contains at least two distinct points) S contains zero-divisors. And if I is infinite then S is not a noetherian ring (if $(a_k) \subseteq I$ is a sequence ($k \in \mathbb{N}$) of points, then the ideals $\mathfrak{a}_k := \mathfrak{v}(I \setminus \{\, a_1, \ldots, a_k \,\})$ form a strictly ascending chain). In this sense S is a *really bad* ring. On the other hand this ring can easily be dealt with. Hence we recommend looking at this ring when searching for counterexamples in general ring theory. Finally if $A \subseteq I$ is a *finite* set then the radical of the ideal $\mathfrak{v}(A)$ is given to be

$$\sqrt{\mathfrak{v}(A)} \;=\; \{\, f \in S \mid \forall\, a \in A : f(a) \in \mathrm{NIL}(R) \,\}$$

Prob in the first equality $\mathfrak{v}(A) \cap \mathfrak{v}(B) = \mathfrak{v}(A \cup B)$ is clear and as $a = 0$ or $b = 0$ implies $ab = 0$ we also get the inclusion $\mathfrak{v}(A)\,\mathfrak{v}(B) \subseteq \mathfrak{v}(A) \cap \mathfrak{v}(B)$. Conversely suppose $h \in \mathfrak{v}(A \cup B)$ and let

$$f(a) := \begin{cases} 0 \text{ if } a \in A \\ 1 \text{ if } a \notin A \end{cases} \quad \text{and} \quad g(a) := \begin{cases} 0 \text{ if } a \in B \\ h(a) \text{ if } a \notin B \end{cases}$$

then $f \in \mathfrak{v}(A)$ and $g \in \mathfrak{v}(B)$ are clear and also $h = fg$. Thus we have proved $\mathfrak{v}(A \cup B) \subseteq \mathfrak{v}(A) \cap \mathfrak{v}(B)$ and thereby finished the first set of identities. In the second equality $\mathfrak{v}(A) + \mathfrak{v}(B) \subseteq \mathfrak{v}(A \cap B)$ is clear. And if we are conversely given any $h \in \mathfrak{v}(A \cap B)$ then let us define

$$f(a) := \begin{cases} 0 \text{ if } a \in A \\ h(a) \text{ if } a \notin A \end{cases} \quad \text{and} \quad g(a) := \begin{cases} h(a) \text{ if } a \in A \setminus B \\ 0 \text{ if } a \notin A \setminus B \end{cases}$$

thereby it is clear that $f \in \mathfrak{v}(A)$ and $g \in \mathfrak{v}(B)$ and an easy distinction of cases truly yields $h = f + g$. Now consider some $f \in S$ with $f^k \in \mathfrak{v}(A)$. That is for any $a \in A$ we get $f(a)^k = f^k(a) = 0$. In other words $f(a) \in \text{NIL}(R)$ for any $a \in A$. Conversely suppose that A is finte and that for any $a \in A$ we get $f(a) \in \text{NIL}(R)$. That is for any $a \in A$ there is some $k(a) \in \mathbb{N}$ such that $f^{k(a)}(a) = 0$. By taking $k := \max\{\, k(a) \mid a \in A \,\}$, we find $f^k \in \mathfrak{v}(A)$.

(1.40) Example:
Sometimes it is helpful to introduce *infinity* as a number. In this example we want to present how this can be done formally. The advantage of this construction is the formal ease by which infinity can be handled, the disadvantage is that the extensions loose may important algebraic properties.

(i) Arithmetic in $\overline{\mathbb{N}} := \mathbb{N} \cup \{\infty\}$: The set $\mathbb{N}$ of natural numbers is well-know. We now pick up a new symbol ∞, which we call *infinity*, and extend the natural order on $\mathbb{N}$ by declaring ∞ to be the maximal element of $\overline{\mathbb{N}}$. That is we define

$$\forall\, k \in \mathbb{N} \quad : \quad k < \infty$$

Also we can extend the usual addition $+$ and multiplication $\cdot$ on $\mathbb{N}$ by defining the addition and multiplication with any $a \in \overline{\mathbb{N}}$ to be

$$\begin{aligned} a + \infty &= \infty + a := \infty \\ a \cdot \infty &= \infty \cdot a := \begin{cases} \infty \text{ if } a \neq 0 \\ 0 \text{ if } a = 0 \end{cases} \end{aligned}$$

Thereby $\overline{\mathbb{N}}$ doesn't loose much properties of $\mathbb{N}$, still $(\overline{\mathbb{N}}, +)$ and $(\overline{\mathbb{N}}, \cdot)$ are commutative monoids, and we also retain the distributivity law between addition and multiplication (it is straightforward to check all this), i.e. for any a, b and $c \in \overline{\mathbb{N}}$ we get:

$$\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c \\ (a + b) \cdot c &= a \cdot c + b \cdot c \end{aligned}$$

The extended set $\overline{\mathbb{N}}$ is mainly used as an index set, if we want to handle finite cases of any finite size and the countably infinite case simultaneously. The next construction has a similar origin: Limits of sequences in $\mathbb{R}$ and volumes in space may be infinitely large. Hence in analysis and measure theory it is nice to have an easy way of dealing with the concept of infinity (without bothering with just how infinite exactly the object is, this is left to cardinality in set theory):

(ii) $(\diamondsuit)$ Arithmetic in $\overline{\mathbb{R}} := \mathbb{R} \cup \{\infty, -\infty\}$: The field $\mathbb{R}$ of real numbers has been introduced earlier in this section and is probably well-known to the reader already. Again we pick up a new symbol ∞, which we call *infinity*, and extend the natural order on $\mathbb{R}$ by making ∞ a maximal and $-\infty$ a minimal element:

$$\forall\, x \in \mathbb{R} \quad : \quad -\infty < x \text{ and } x < \infty$$

Again we extend the usual addition $+$ and multiplication $\cdot$ by defining the addition and multiplication with ∞ resp. with $-\infty$

$$\begin{array}{lcccl}
\forall\, a \in \mathbb{R} \cup \{\infty\} & : & a + \infty & = & \infty + a & := & \infty \\
\forall\, a \in \mathbb{R} \cup \{-\infty\} & : & a - \infty & = & -\infty + a & := & -\infty \\
\forall\, a \in \mathbb{R} \setminus \{0\} & : & a \cdot \infty & = & \infty \cdot a & := & \begin{cases} \infty \text{ if } a > 0 \\ -\infty \text{ if } a < 0 \end{cases} \\
\forall\, a \in \mathbb{R} \setminus \{0\} & : & a \cdot (-\infty) & = & (-\infty) \cdot a & := & \begin{cases} -\infty \text{ if } a > 0 \\ \infty \text{ if } a < 0 \end{cases}
\end{array}$$

Note that we did *neither* define $\infty + (-\infty)$ *nor* did we define $0 \cdot \infty$. Hence the set $\overline{\mathbb{R}}$ is no algebraic structure, as the operations $+$ and $\cdot$ are not fully defined! In fact any such definition would only result in contradictions: Suppose we had $\infty - \infty = 0$, as could have been expected, then since $1 \cdot \infty = \infty = 2 \cdot \infty$ we had $\infty = (2-1) \cdot \infty = \infty - \infty = 0$. Hence $\infty = 0$ wouldn't be a new element. In conclusion we just *cannot* define $\infty + (-\infty)$ or $0 \cdot \infty$, these terms have to be evaded - that is they may not occur within a computation. This is the one and only reason why computations with infinity have to be handled with great care.

The reason behind this is an analytic one: Take a look at the sequence $(n) = (0, 1, 2, 3, \dots) \subseteq \mathbb{R}$. We would like to write $(n) \to \infty$, as this sequence does not converge in $\mathbb{R}$ but increases strictly monotonous. Yet the difference of two determined divergent sequences can be just about anything: For any $a \in \mathbb{R}$ we get $(n + a) - (n) = (a) \to a$, whereas $(n^2) - (n) \to \infty$. Thus the result of $\infty - \infty$ is completely uncontrolled, as the limit of the difference of two sequences may be just about anything. The same is true for $\infty \cdot 0$. For example $(n) \cdot (1/n) = (1) \to 1$ converges trivially. Yet $(n^2) \cdot (1/n) = (n) \to \infty$ and even $(n) \cdot (1/n^2) = (1/n) \to 0$. Thus the limit can take any number or $\pm\infty$ again and therefore it makes no sense to fix a value for $\infty \cdot 0$.

1.5 First Concepts

Some Combinatorics

In the following proposition we want to establish some basic computational rules, that are valid in arbitrary rings. But in order to do this we first have to recall some elementary facts from combinatorics: First consider a set containing $1 \leq k \in \mathbb{N}$ elements. If we want to put a linear order to this set, we have to choose some first element. To do this there are k possibilities. We commence by choosing the second element - now having $(k-1)$ possibilities, and so on. Thus we end up with a number of linear orders on this set that equals $k!$ the *faculty* of k, that is defined to be

$$\begin{aligned} k! &:= \#\{\, \sigma : 1 \dots k \to 1 \dots k \mid \sigma \text{ bijective} \,\} \\ &= k \cdot (k-1) \cdots 2 \cdot 1 \end{aligned}$$

If $k = 0$ we specifically define $0! := 1$. Next we consider a set containing $n \in \mathbb{N}$ elements. If we want to select a subset I of precisely $k \in 0 \dots n$ elements we have to start by choosing a first element (n possibilities). In the next step we may only choose from $(n-1)$ elements and so on. We end with the k-th choice, for which we still have $n-k+1$ numbers to choose from, left. But as a subset does not depend on the order of its elements, we still have to divide by $k!$ - the number of linear orders on I. Altogether we end up with

$$\begin{aligned} \binom{n}{k} &:= \#\{\, I \subseteq 1 \dots n \mid \#I = k \,\} \\ &= \frac{n}{k} \cdot \frac{n-1}{k-1} \cdots \frac{n-k+1}{1} \\ &= \frac{n!}{k!\,(n-k)!} \end{aligned}$$

Note that this definition also works out in the case $n = 0$ and $k = 0$ (in which the *binomial coefficient* $(n\ k)$ equals one. That is we get $(n\ 0) = 1 = (n\ n)$. Also it is clear (by looking at the formular above), that $(n\ k)$ is just the same, as $(n\ n-k)$. This makes sense: To gather I you can either pick out the elements of I or take away all $k \notin I$, so that only I is left. Furthermore the binomial coefficents satisfy a famous recursion formula, which is the reason behind *Pascal's triangle*

$$\begin{aligned} \binom{n}{n-k} &= \binom{n}{k} \\ \binom{n+1}{k} &= \binom{n}{k} + \binom{n}{k-1} \end{aligned}$$

Finally consider some *multi-index* $\alpha = (\alpha_1, \dots, \alpha_k) \in \mathbb{N}^k$. Then it will be useful to introduce the following notations (where the latter will only be used, for $n := |\alpha|$)

$$\begin{aligned} |\alpha| &:= \alpha_1 + \cdots + \alpha_k \\ \alpha! &:= (\alpha_1!) \cdot \ldots \cdot (\alpha_k!) \\ \binom{n}{\alpha} &:= \frac{n!}{\alpha!} \end{aligned}$$

(1.41) Proposition: (viz. 725)

- Let $(R,+,\cdot)$ be any semi-ring and consider arbitrary elements $a, b \in R$ of R. Then the following computational rules hold true

$$\begin{aligned} 0 &= -0 \\ a0 &= 0 = 0a \\ (-a)b &= -(ab) = a(-b) \\ (-a)(-b) &= ab \end{aligned}$$

- If now $a_1, \ldots, a_m \in R$ and $b_1, \ldots, n_n \in R$ are finitely many, arbitrary elements of R, then we also obtain the *general rule of distributivity*

$$\left(\sum_{i=1}^{m} a_i\right)\left(\sum_{j=1}^{n} b_j\right) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_i b_j$$

 And if $J(1), \ldots, J(n)$ are finite index sets (where $1 \leq n \in \mathbb{N}$) and $a(i,j) \in R$ for any $i \in 1 \ldots n$, $j \in J(i)$ then we let $J := J(1) \times \cdots \times J(n)$ (and $j = (j_1, \ldots, j_n) \in J$) and thereby obtain

$$\prod_{i=1}^{n} \sum_{j_i \in J(i)} a(i,j_i) = \sum_{j \in J} \prod_{i=1}^{n} a(i,j_i)$$

- Now suppose $(R,+,\cdot)$ is a ring, $n \in \mathbb{N}$ and $a, b \in R$ are elements, that mutually commute (that is $ab = ba$), then we get the *binomial rule*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

 And if $(R,+,\cdot)$ even is a commutative ring $a_1, \ldots, a_k \in R$ are finitely many elements and $n \in \mathbb{N}$ then we even get the following *polynomial rule*, where the sum runs over all multi-indexes $\alpha \in \mathbb{N}^k$ that satisfy $|\alpha| = \alpha_1 + \cdots + \alpha_k = n$. And a^α abbreviates $a^\alpha := (a_1)^{\alpha_1} \cdots (a_k)^{\alpha_k}$

$$(a_1 + \cdots + a_k)^n = \sum_{|\alpha|=n} \binom{n}{\alpha} a^\alpha$$

(1.42) Remark:
Thus there are many computational rules that hold true for arbitrary rings. However there also are some exceptions to integer (or even real) arithmetic. E.g. we are *not* allowed to deduce $a = 0$ or $b = 0$ from $ab = 0$. As a counterexample regard $a = 2 + 6\mathbb{Z}$ and $b = 3 + 6\mathbb{Z}$ in $\mathbb{Z}_6$. A special case of this is the following: We may *not* deduce $a = 0$ from $a = -a$. As a counterexample regard $a = 1 + 2\mathbb{Z}$ in $\mathbb{Z}_2$.

(1.43) Remark:
An exceptional role pays the **zero-ring** $R = \{0\}$, it clearly is a commutative ring (under the trivial operations) that would even satisfy condition (F). But it is the only ring in which $0 = 1$. More formally we've got the equivalence

$$R = \{0\} \quad \Longleftrightarrow \quad 0 = 1$$

[as $\Longrightarrow$ is clear and in the converse direction regard $a = 1a = 0a = 0$]. This equality $0 = 1$ will lead to some peculiarities however. This is precisely why we required $0 \neq 1$ for skew-fields and fields. And several theorems will require R to be not the zero-ring, which we will abbreviate by $R \neq 0$.

(1.44) Remark: (viz. 727)
As a neat little application of the binomial rule let us present a generalization of the recursion formula for the binomial coefficients: Regarding the expression $(x+y)^n = (x+y)^k(x+y)^{n-k}$ in $\mathbb{Z}[x,y]$ and comparing coefficients, one easily verifies, that for any $k, n \in \mathbb{N}$ and any $r \in 0 \ldots k$ we get

$$\sum_{i=0}^{r} \binom{k}{i}\binom{n-k}{r-i} \;=\; \binom{n}{r}$$

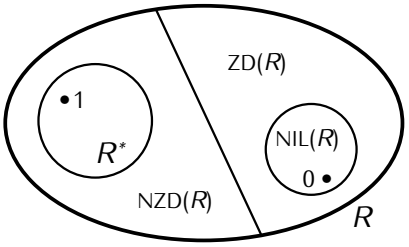
(1.45) Definition: (viz. 728)
Let $(R,+,\cdot)$ be any semi-ring and $b \in R$ be any element of R. Then we define the sets $\text{ZD}(R)$ of **zero-divisors**, $\text{NZD}(R)$ of **non-zero-divisors**, the **nil-radical** $\text{NIL}(R)$ and the **annihilator** $\text{ann}(b)$ of b to be

$$\begin{aligned}
\text{ZD}(R) &:= \{\, a \in R \mid \exists\, b \in R \;:\; b \neq 0 \text{ and } ab = 0 \,\} \\
\text{NZD}(R) &:= \{\, a \in R \mid \forall\, b \in R \;:\; ab = 0 \implies b = 0 \,\} \\
\text{NIL}(R) &:= \left\{\, a \in R \mid \exists\, k \in \mathbb{N} \;:\; a^k = 0 \,\right\} \\
\text{ann}(b) &:= \{\, a \in R \mid ab = 0 \,\}
\end{aligned}$$

We sometimes also write $\text{ann}_R(b)$ instead of $\text{ann}(b)$ to emphasize the ring $\text{ann}_R(b) \subseteq R$ is taken in. An element $a \in \text{NIL}(R)$ contained in the nil-radical is also said to be *nilpotent*. If now R even is a ring we define the set R^* of **units** (or *invertible* elements) and the set $R^\bullet$ of *relevant* elements of R

$$\begin{aligned}
R^* &:= \{\, a \in R \mid \exists\, b \in R : ab = 1 = ba \,\} \\
R^\bullet &:= R \setminus \left(\{0\} \cup R^*\right)
\end{aligned}$$

The following Venn-diagramm illustrates the situation how these sets relate to each other. Algebraically this will be formulated and proved in (1.47)



And $(R,+,\cdot)$ is said to be **integral**, iff it does not contain any non-zero zero-divisors, that is iff it satisfies one of the following five equivalent statements

(a) $\text{ZD}(R) \;=\; \{0\}$

(b) for any a, b and $c \in R$ such that $a \neq 0$ we get $ab = ac \implies b = c$

(b') for any a, b and $c \in R$ such that $c \neq 0$ we get $ac = bc \implies a = b$

(c) for any a, $b \in R$ such that $a \neq 0$ we get $ab = a \implies b = 1$

(c') for any a, $b \in R$ such that $b \neq 0$ we get $ab = b \implies a = 1$

Now $(R,+,\cdot)$ is said to be an **integral domain**, iff it is a commutative ring that also is non-zero $R \neq 0$ and satisfies $\text{ZD}(R) = \{0\}$.

(1.46) Remark:

- Consider any semi-ring $(R,+,\cdot)$, two elements a, $b \in R$ and a non-zero-divisor $n \in \text{NZD}(R)$. Then $a = b$ is equivalent to $na = nb$, formally

$$a = b \quad\iff\quad na = nb$$

 Prob the direction " $\implies$ " is clear, and if $na = nb$ then $n(a-b) = 0$ which implies $a - b = 0$ (and hence $a = b$), since n is a non-zero-divisor.

- Let $(R,+,\cdot)$ be a ring, $a \in R$ be any element and $n \in \text{NZD}(R)$ be a non-zero-divisor. Then we obtain the implication

$$na = 1 \quad\implies\quad an = 1$$

 Prob since $n(an) = (na)n = n$ and hence $n(an-1) = 0$. But as n is a non-zero-divisor this implies $an - 1 = 0$ and hence $an = 1$.

- Consider a commutative ring $(R,+,\cdot)$ and finitely many elements $a_1, \ldots, a_n \in R$. Let $u \in R$ be the product of these a_i, that is $u := a_1 \ldots a_n \in R$, then we obtain the implication

$$u \in R^* \quad\implies\quad a_1, \ldots, a_n \in R^*$$

 Prob choose any $j \in 1 \ldots n$ and let $\widehat{a}_j := \prod_{i \neq i} a_i$, e.g. $\widehat{a}_1 := a_2 \ldots a_n$. Then by construction we get $1 = u^{-1}(a_1 \ldots a_n) = (u^{-1}\widehat{a}_j)a_j$. And hence we see $a_j \in R^*$ with inverse $a_j^{-1} = u^{-1}\widehat{a}_j$.

- ($\diamondsuit$) For an R-module M over a ring $(R,+,\cdot)$ we will generalize this concept in the following way: We will define the set of *zero-divisors* of M to be the set of all $a \in R$ that turn $x \in M$ with $x \neq 0$ into $ax = 0$ under scalar multiplication

$$\text{ZD}_R(M) \;:=\; \{\, a \in R \mid \exists\, x \in M \,:\, x \neq 0 \text{ and } ax = 0 \,\}$$

 Then $\text{ZD}_R(R) = \text{ZD}(R)$ if we consider R as an R-module. And if $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ is an ideal, if we consider $M = R/\mathfrak{a}$ as an R-module, we find $\text{ZD}_R(R/\mathfrak{a}) = \{\, a \in R \mid \exists\, b \in R\; b \notin \mathfrak{a} \text{ and } ab \in \mathfrak{a} \,\}$ such that $\text{ZD}(R/\mathfrak{a}) = \{\, a + \mathfrak{a} \mid a \in \text{ZD}_R(R/\mathfrak{a}) \,\}$. Refer to (2.89) for more comments on this.

- If $(R,+,\cdot)$ is a skew-field, then R already is integral (i.e. $\mathrm{zd}(R)=\{0\}$) and allows division: That is any two elements $a, b \in R$ with $a \neq 0$ are connectet via multiplication, in the following sense:

$$\exists!\, u,v \in R \;\; : \;\; ua = b \;\text{ and }\; av = b$$

 Prob since $a \neq 0$ and R is a skew-field there is some $i \in R$ such that $ai = 1 = ia$. Now suppose $ab = 0$, then $b = (ia)b = i(ab) = 0$ and hence $a \in \mathrm{nzd}(R)$. This proves $\mathrm{zd}(R) = \{0\}$. Again, given $a, b \in R$ with $a \neq 0$ choose $i \in R$ such that $ai = 1 = ia$ and let $u := bi$ and $v := ib$. Then $ua = (bi)a = b(ia) = b$ and $av = a(ib) = (ai)b = b$. Now suppose $u', v' \in R$ with $ua = b = u'a$ and $av = b = av'$. Then $a(v - v') = 0$ but as $a \neq 0$ we have seen that this implies $v - v' = 0$ and hence $v = v'$. Likewise $(u - u')a = 0$ implies $u = u'$.

The sets of zero-divisors $\mathrm{zd}(R)$ and of relevant elements $R^\bullet$ rarely carry any noteworthy algebraic structure. Yet the units R^* form a group, the non-zero-divisors $\mathrm{nzd}(R)$ are multiplicatively closed, the nil-radical $\mathrm{nil}(R)$ is an (even perfect) ideal of R and the annihilator $\mathrm{ann}(b)$ of some element $b \in R$ is a sub-module. Though we have not introduced these structures yet, we would like to present a formal proposition (and proof) of these facts already.

(1.47) Proposition: (viz. 728) $(\diamondsuit)$

(i) Let $(R,+,\cdot)$ be any semi-ring, then R is the disjoint union of its zero-divisors and non-zero divisors

$$\mathrm{nzd}(R) \;\; = \;\; R \setminus \mathrm{zd}(R)$$

(ii) In any non-zero ($R \neq 0$) ring $(R,+,\cdot)$ the nilradical is contained in the set of zero-divisors. And the zero-divisors are likewise contained in non-units of R. That is we've got the inclusions

$$\mathrm{nil}(R) \;\; \subseteq \;\; \mathrm{zd}(R) \;\; \subseteq \;\; R \setminus R^*$$

(iii) Let $(R,+,\cdot)$ be any semi-ring, then the set $\mathrm{nzd}(R) \subseteq R$ of non-zero-divisors of R is multiplicatively closed, that is we get it satisfies the following two properties

$$1 \;\; \in \;\; \mathrm{nzd}(R)$$

$$a, b \in \mathrm{nzd}(R) \;\; \Longrightarrow \;\; ab \in \mathrm{nzd}(R)$$

(iv) Consider any ring $(R,+,\cdot)$, then $(R^*,\cdot)$ is a group (where $\cdot$ denotes the multiplication of R), called the *multiplicative group* of R.

(v) If $(R,+,\cdot)$ is any ring then R is a skew-field if and only if the multiplicative group of R consists precisely of the non-zero elements. That is we find the equivalence, of

$$R \text{ skew-field} \;\; \Longleftrightarrow \;\; R^* = R \setminus \{0\}$$

(vi) If $(R,+,\cdot)$ is a commutative ring, then the nil-radical is an ideal of R. Symbolically: $\mathrm{nil}(R) \trianglelefteq_{\mathrm{i}} R$.

(vii) Let $(R,+,\cdot)$ be any ring and $b \in R$ an element of R. Then the annihilator $\mathrm{ann}(b)$ is a left-ideal (i.e. a sub-module) of R. Symbolically $\mathrm{ann}(b) \leq_{\mathsf{m}} R$.

(viii) Let $(R,+,\cdot)$ be a commutative ring and $u \in R^*$ be a unit of R. Then $u + \mathrm{NIL}(R) \subseteq R^*$. To be precise, if $a \in R$ with $a^n = 0$ then we get

$$(u+a)^{-1} \;=\; \sum_{k=0}^{n-1} (-1)^k a^k u^{-k-1}$$

(ix) If $(R,+,\cdot)$ is an integral domain, $F := \mathrm{QUOT}(R)$ its quotient field and $E \leq_{\mathsf{f}} F$ is a sub-field of F, then we get the equivalence of

$$R \subseteq E \iff E = F$$

(1.48) Example:
We present a somewhat advanced example that builds upon some results from linear algebra. Let us regard the ring $R := \mathrm{mat}_2(\mathbb{Z})$ of (2×2)-matrices over the integers. We will need the notions of the *determinant*, *trace* and *adjoint matrix* of a matrix

$$\begin{aligned}
\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} &:= ad - bc \in \mathbb{Z} \\
\mathrm{tr} \begin{pmatrix} a & b \\ c & d \end{pmatrix} &:= a + d \in \mathbb{Z} \\
\begin{pmatrix} a & b \\ c & d \end{pmatrix}^\sharp &:= \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}
\end{aligned}$$

Then we can explicitly determine which matrices are *invertible* (that is units), which are zero-divisors and which are nil-potent. We find

$$\begin{aligned}
R^* &= \{\, A \in R \mid \det A = \pm 1 \,\} \\
\mathrm{ZD}(R) &= \{\, A \in R \mid \det A = 0 \,\} \\
\mathrm{NIL}(R) &= \{\, A \in R \mid \det A = \mathrm{tr} A = 0 \,\}
\end{aligned}$$

($\diamondsuit$) Prob first note that an easy computation yields $AA^\sharp = (\det A)\mathbb{1} = A^\sharp A$. Hence if A is invertible, then $A^{-1} = (\det A)^{-1} A^\sharp$. Thus A is invertible if and only if $\det A$ is a unit (in $\mathbb{Z}$), but as the units of $\mathbb{Z}$ are given to be $\mathbb{Z}^* = \{\pm 1\}$ this already is the first identity. For the second identity we begin with $\det A = 0$. Then $AA^\sharp = (\det A)\mathbb{1} = 0$ and hence A is a zero-divisor. Conversely suppose that $A \in \mathrm{ZD}(R)$ is a zero-divisor, then $AB = 0$ for some $B \neq 0$ and hence $(\det A)B = A^\sharp AB = 0$. But as B is non-zero this implies $\det A = 0$. Finally if $\det A = 0$ then an easy computation shows $A^2 = (\mathrm{tr} A)A$, thus if also $\mathrm{tr} A = 0$ then $A^2 = 0$ and hence $A \in \mathrm{NIL}(R)$. And if conversely $A \in \mathrm{NIL}(R) \subseteq \mathrm{ZD}(R)$, then $\det A = 0$ and hence (by induction on n) $A^n = (\mathrm{tr} A)^{n-1} A$. As A is nilpotent there is some $1 \leq n \in \mathbb{N}$ such that $0 = A^n = (\mathrm{tr} A)^{n-1} A$ and hence $\mathrm{tr} A \in \mathrm{NIL}(\mathbb{Z}) = \{0\}$.

($\diamondsuit$) The following proposition is a classical topic, called *partial fraction decomposition* of rational fractions $f/g \in E(t)$ over some base field E. It only is loosely connected to the rest of this text and uses some notions, that probably are known to the reader, but - from a formal point of view - will be introduced in chapter 7 only. So you might want to skip it, for now.

(1.49) Proposition: (viz. 808)
Let $(E,+,\cdot)$ be any field, consider two polynomials f and $g \in E[t]$ and denote the quotient field of $E[t]$ (called the field of *rational fractions*) by $E(t)$ [refer to (1.31) for a construction]

(i) If $x \in E$ is not a root $g(x) \neq 0$ of g, then there are a constant $c \in E$ and a polynomial $h \in E[t]$ such that for any $k \in \mathbb{N}$ the following equality in $E(t)$ holds true

$$\frac{f(t)}{(t-x)^k g(t)} \;=\; \frac{c}{(t-x)^k} + \frac{h(t)}{(t-x)^{k-1} g(t)}$$

Thereby the constant c and the polynomial h are uniquely determined, to be the following [note that $t-x$ divides $f(t)-cg(t)$ such that h is a polynomial not only a rational fraction]

$$c \;=\; f(x)g(x)^{-1} \quad \text{and} \quad h(t) \;=\; \frac{f(t)-cg(t)}{t-x}$$

(ii) Suppose that g *splits* over E, that is $g \neq 0$ and there are pairwise distinct *roots* $x_i \in E$ and powers $1 \leq k_i \in \mathbb{N}$, such that letting $b := \mathrm{lc}(g)$ we can write g in the form

$$g(t) \;=\; b\,(t-x_1)^{k_1} \ldots (t-x_r)^{k_r}$$

Further assume that f is of lesser degree $\deg(f) < \deg(g)$ than g, then there are uniquely determined coefficients $c_{i,j} \in E$ (where $i \in 1 \ldots r$ and $j \in 1 \ldots k_i$) such that in $E(t)$ we get

$$\frac{f(t)}{g(t)} \;=\; \sum_{i=1}^{r} \sum_{j=1}^{k_i} \frac{c_{i,j}}{(t-x_i)^j}$$

Nota let $n := \deg(g)$, then clearly $\{\, f(t)/g(t) \mid f \in E[t], \deg(f) < n \,\} \subseteq E(t)$ is an E-vector space. And its canonical basis is given to be $\{\, x^k/g(t) \mid k \in 0 \ldots n \,\}$. Now (ii) can be reformulated, as: Also $\{\, 1/(t-x_i)^j \mid i \in 1 \ldots r, j \in 1 \ldots k_i \,\}$ is a basis of this vector space.

Nota if $\deg(f) \geq \deg(g)$ we may use division with remainder - refer to (2.67) - first, to write $f(t)$ in the form $f = qg + r$ for some polynomials $q(t)$, $r(t) \in E[t]$ with $\deg(r) < \deg(g)$. Then $f/g = q + r/g$ and we may apply (ii) here to r/g to finally get

$$\frac{f(t)}{g(t)} \;=\; q(t) + \sum_{i=1}^{r} \sum_{j=1}^{k_i} \frac{c_{i,j}}{(t-x_i)^j}$$

1.6 Ideals

(1.50) Definition:

- Let $(R,+,\cdot)$ be a semi-ring and $P \subseteq R$ a subset. Then P is said to be a **sub-semi-ring** of R (abbreviated by $P \leq_s R$), iff for any $a, b \in R$ we get

 (1) $0 \in P$

 (2) $a, b \in P \implies a+b \in P$

 (3) $a \in P \implies -a \in P$

 (4) $a, b \in P \implies ab \in P$

- And if $(R,+,\cdot)$ is a ring having the unit element 1, then a subset $P \subseteq R$ is called a **sub-ring** of R (abbreviated by $P \leq_r R$), iff we have

 (S) $P \leq_s R$

 (5) $1 \in P$

- Finally if $(R,+,\cdot)$ even is a (skew)field, then a subset $P \subseteq R$ is said to be a **sub-(skew)field** of R (abbreviated $P \leq_f R$), iff for any $a \in R$ we get

 (R) $P \leq_r R$

 (6) $0 \neq a \in P \implies a^{-1} \in P$

- Let $(R,+,\cdot)$ be a semi-ring again, then a subset $\mathfrak{a} \subseteq R$ is said to be a **left-ideal** (or **sub-module**) of R (abbreviated by $\mathfrak{a} \leq_m R$), iff for any $a, b \in R$ we get

 (1) $0 \in \mathfrak{a}$

 (2) $a, b \in \mathfrak{a} \implies a+b \in \mathfrak{a}$

 (3) $a \in \mathfrak{a} \implies -a \in \mathfrak{a}$

 (4) $a \in \mathfrak{a}, b \in R \implies ba \in \mathfrak{a}$

 The subset $\mathfrak{a} \subseteq R$ is said to be an **ideal** of R (abbreviated by $\mathfrak{a} \trianglelefteq_i R$), iff for any $a, b \in R$ we get

 (M) $\mathfrak{a} \leq_m R$

 (5) $a \in \mathfrak{a}, b \in R \implies ab \in \mathfrak{a}$

- We will sometimes use the set of all sub-rings (of a ring R), the set of all sub(skew)fields (of a (skew)field R), resp. the set of all (left-)ideals (of a semi-ring R) - these will be denoted, by

$$\begin{aligned}
\mathrm{Subr}(R) &:= \{ P \subseteq R \mid P \leq_r R \} \\
\mathrm{Subf}(R) &:= \{ P \subseteq R \mid P \leq_f R \} \\
\mathrm{Subm}(R) &:= \{ \mathfrak{a} \subseteq R \mid \mathfrak{a} \leq_m R \} \\
\mathrm{Ideal}(R) &:= \{ \mathfrak{a} \subseteq R \mid \mathfrak{a} \trianglelefteq_i R \}
\end{aligned}$$

(1.51) Remark:

- Consider any semi-ring $(R,+,\cdot)$ and an arbitrary sub-semi-ring $P \leq_s R$ of R. Then we would like to emphasize, that the notion of a sub-semi-ring was defined in such a way that the addition $+$ and multiplication $\cdot$ of R induces the like operations on P

$$\begin{aligned} +\big|_P &: P \times P \to P \;:\; (a,b) \mapsto a+b \\ \cdot\big|_P &: P \times P \to P \;:\; (a,b) \mapsto ab \end{aligned}$$

 And thereby $(P, +\big|_P, \cdot\big|_P)$ becomes a semi-ring again (clearly all the properties of such are inherited from R). And in complete analogy we find that sub-rings of rings are rings again and sub(skew)fields of (skew)fields are (skew)fields again, under the induced operations.

 Nota as $+\big|_P$ and $\cdot\big|_P$ are just restrictions of the respective functions $+$ and $\cdot$ on R, we will not distinguish between $+\big|_P$ and $+$ respectively between $\cdot\big|_P$ and $\cdot$. That is we will speak of the semi-ring $(P,+,\cdot)$, where $+$ and $\cdot$ here are understood to be the restricted operations $+\big|_P$ and $\cdot\big|_P$ acting on $P \times P$, respectively.

- Beware: It is possible, that a sub-semi-ring $P \leq_s R$ is a ring $(P,+,\cdot)$ under the induced operations, but *no* sub-ring of R. E.g. consider $R := \mathbb{Z} \times \mathbb{Z}$ under the point-wise operations and $P := \mathbb{Z} \times \{0\} \subseteq R$. Then $P \leq_s R$ is a sub-semi-ring. But it is no sub-ring, as the unit element $(1,1) \in R$ of R is *not* contained $(1,1) \notin P$ in P. Nevertheless P has a unit-element, namely $(1,0) \in P$ and hence is a ring in itself.

- If $(R,+,\cdot)$ is a *ring*, then property (3) of left-ideals is redundant, it already follows from property (4) by letting $b := -1$. We only require (3) in case of a *semi*-ring R.

- Let $(R,+,\cdot)$ be a semi-ring, then trivially any left-ideal $\mathfrak{a}$ of R already is a sub-semi-ring. Formally put for any subset $\mathfrak{a} \subseteq R$ we get the implication

$$\mathfrak{a} \leq_m R \implies \mathfrak{a} \leq_s R$$

- Consider a commutative semi-ring $(R,+,\cdot)$, then the property (4) of left-ideals already implies property (5) of ideals, due to commutativity. That is in a *commutative* semi-ring R we find the following equivalence for any subset $\mathfrak{a} \subseteq R$

$$\mathfrak{a} \leq_m R \iff \mathfrak{a} \trianglelefteq_i R$$

- Now let $(R,+,\cdot)$ be any ring and let $\mathfrak{a} \leq_m R$ be a left-ideal of R. Then clearly clearly $1 \in \mathfrak{a}$ is just the same, as $a = R$. We will call $\mathfrak{a}$ a **proper** left-ideal, iff $\mathfrak{a} \neq R$. Formally put

$$\mathfrak{a} = R \iff 1 \in \mathfrak{a}$$

 Prob " $\implies$ " is clear, as $1 \in R$ and if conversely $1 \in \mathfrak{a}$ then due to property (4) we have $a = a1 \in \mathfrak{a}$ for any $a \in R$. Hence $R \subseteq \mathfrak{a} \subseteq R$, such that $\mathfrak{a} = R$.

- Consider any semi-ring $(R, +, \cdot)$ and some element $a \in R$. Then we obtain a left-ideal Ra in R (called the **principal ideal** of a), by letting

$$Ra \;:=\; \{\, ba \mid b \in R \,\} \quad \leq_{\mathfrak{m}} \quad R$$

 Prob clearly $0 = 0a \in Ra$ and if ba and $ca \in R$, then we see that $ba + ca = (b + c)a \in Ra$ and $-(ba) = (-b)a \in Ra$. Finally we have $c(ba) = (cb)a \in Ra$ for any $c \in R$.

- In a *commutative* semi-ring $(R, +, \cdot)$ (where $a \in R$ again) we clearly get $Ra = aR$, where the latter is defined to be the following subset, which already is an ideal of R

$$aR \;:=\; \{\, ab \mid b \in R \,\} \quad \trianglelefteq_{\mathfrak{i}} \quad R$$

 And as R is commutative $Ra = aR$ already is an ideal of R. And it is customary to take to aR instead of Ra, in this case. We will later see (cf. section 2.7), that $\mathbb{Z}$ is a PID - that is *every* ideal of $\mathbb{Z}$ is of the form $a\mathbb{Z}$ for some $a \in \mathbb{Z}$. Formally that is

$$\mathrm{Ideal}(\mathbb{Z}) \;=\; \{\, a\mathbb{Z} \mid a \in \mathbb{Z} \,\}$$

- In any semi-ring $(R, +, \cdot)$ we always have the *trivial* ideals $\{0\}$ and $R \trianglelefteq_{\mathfrak{i}} R$. If R is a skew-field, then these even are the only ideals of R, that is

$$R \text{ skew-field} \quad \Longrightarrow \quad \mathrm{Subm}(R) = \{\, \{0\}, R \,\}$$

 Nota it is customary to denote the ideal $\{0\}$ by 0 again. This is an abuse of notation, as 0 also is the zero-element of R. Do not mix these up and beware $0 \in 0$, as hereby the first is $0 \in R$ and the second is $0 \trianglelefteq_{\mathfrak{i}} R$. Prob let $\mathfrak{a} \leq_{\mathfrak{m}} R$ be any left-ideal of R, if there is some $0 \neq a \in \mathfrak{a}$ then $a^{-1} \in R$ and hence $1 = a^{-1}a \in \mathfrak{a}$. And from this we get $\mathfrak{a} = R$, by the reasoning above.

- Now consider some non-zero ($R \neq 0$) commutative ring $(R, +, \cdot)$. Then we even get: R is a field if and only if the only ideals of R are the trivial ones. That is equivalent are

$$R \text{ field} \quad \Longleftrightarrow \quad \mathrm{Ideal}(R) = \{\, \{0\}, R \,\}$$

 Prob " $\Longrightarrow$ " has already been shown above, for " $\Longleftarrow$ " regard any $0 \neq a \in R$, then $aR \trianglelefteq_{\mathfrak{i}} R$ is an ideal of R. But as $aR \neq \{0\}$ this only leaves $aR = R$ and hence there is some $i \in R$ such that $ai = 1$, which means $i = a^{-1}$. Altogether R is a field.

- We could have introduced a dual notion of a left-ideal - a so-called *right-ideal*. This is a subset $\mathfrak{a} \subseteq R$ such that the properties (1), (2), (3) and (5) of (left-)ideals hold true. That is we have replaced (4) by (5). However this would lead to a completely analogous theory. Also refer to section 3.1 for a little more comments on this.

(1.52) Lemma: (viz. 730)
For the moment being let $\star$ abbreviate any one of the words *semi-ring*, *ring*, *skew-field* or *field* and let $(R,+,\cdot)$ be a $\star$. Further consider an arbitrary family (where $i \in I \neq \emptyset$) $P_i \subseteq R$ of sub-$\star$s of R. Then the intersection P_i is a sub-$\star$ of R again

$$\bigcap_{i\in I} P_i \quad \subseteq \quad R \quad \text{is a sub-}\star$$

Likewise let us abbreviate by $\star$ the word *left-ideal* or the word *ideal*. Now suppose $(R,+,\cdot)$ is a semi-ring and consider an arbitrary family (where $i \in I \neq \emptyset$) $\mathfrak{a}_i \subseteq R$ of $\star$s of R. Then the intersection of the $\mathfrak{a}_i$ is a $\star$ of R again

$$\bigcap_{i\in I} \mathfrak{a}_i \quad \subseteq \quad R \quad \text{is a } \star$$

The proof of this lemma is an easy, straightforward verification of the properties of a (sub-)$\star$ in all the separate cases. But though this is most easy it has far-reaching consequences. Whenever we are given a subset $X \subseteq R$ we may consider the smallest $\star$ of R containing X. Just take the intersection over all $\star$s containing X (this is possible since at least R is a $\star$ with $X \subseteq R$). The following definition formalizes this idea. And it is not much of a surprise, that this smallest $\star$ then can be described explicitly by taking all the elements of X and performing all the operations allowed for a $\star$.

(1.53) Definition:
Let now $(R,+,\cdot)$ be a semi-ring and consider an arbitrary subset $X \subseteq R$ of R. Then the above lemma allows us to introduce the sub-semi-ring, left-ideal, resp. ideal **generated** by X to be the intersection of all such containing X

$$\begin{aligned}
\langle X\rangle_{\mathsf{s}} &:= \bigcap\{\, P \subseteq R \mid X \subseteq P \leq_{\mathsf{s}} R\,\}\\
\langle X\rangle_{\mathsf{m}} &:= \bigcap\{\, \mathfrak{a} \subseteq R \mid X \subseteq \mathfrak{a} \leq_{\mathsf{m}} R\,\}\\
\langle X\rangle_{\mathsf{i}} &:= \bigcap\{\, \mathfrak{a} \subseteq R \mid X \subseteq \mathfrak{a} \trianglelefteq_{\mathsf{i}} R\,\}
\end{aligned}$$

Likewise if R even is a ring (or (skew)field) we may define the sub-ring (or sub-(skew)field respectively) to be the intersection of all such containing X

$$\begin{aligned}
\langle X\rangle_{\mathsf{r}} &:= \bigcap\{\, P \subseteq R \mid X \subseteq P \leq_{\mathsf{r}} R\,\}\\
\langle X\rangle_{\mathsf{f}} &:= \bigcap\{\, P \subseteq R \mid X \subseteq P \leq_{\mathsf{f}} R\,\}
\end{aligned}$$

Nota in case that there may be any doubt concerning the semi-ring X is contained in (e.g. $X \subseteq R \subseteq S$) we emphasize the semi-ring R used in this construction by writing $\langle X \subseteq R\rangle_{\mathsf{i}}$ or $\langle X\rangle_{\mathsf{i}} \trianglelefteq_{\mathsf{i}} R$ or even $R\langle X\rangle_{\mathsf{i}}$.

(1.54) Remark:
In case $X = \emptyset$ it is clear that $\{0\}$ is an ideal containing X. And as 0 is contained in any other ideal (even sub-semiring) of R we find

$$\langle\emptyset\rangle_{\mathsf{s}} \;=\; \langle\emptyset\rangle_{\mathsf{m}} \;=\; \langle\emptyset\rangle_{\mathsf{i}} \;=\; \{0\}$$

The case of the sub-ring resp. sub(skew)field generated by $\emptyset$ usually is less trivial however. Let us regard the case $R = \mathbb{Q}$ for example. As any sub-ring has to contain 1 and allow sums and negatives, we find that $\mathbb{Z} = \langle\emptyset\rangle_{\mathsf{r}} \subseteq \mathbb{Q}$. And as a sub-field even allows to take inverses we find $\mathbb{Q} = \langle\emptyset\rangle_{\mathsf{f}} \subseteq \mathbb{Q}$. However in $\mathbb{C}$ we also get $\mathbb{Q} = \langle\emptyset\rangle_{\mathsf{f}} \subseteq \mathbb{C}$ only. Hence the intersection of all sub-rings resp. all sub(skew)fields deserves a special name, it is called the **prime-ring** resp. **prime-(skew-)field** of R

$$\begin{aligned}\langle\emptyset\rangle_{\mathsf{r}} &= \bigcap\{\, P \subseteq R \mid P \leq_{\mathsf{r}} R \,\}\\ \langle\emptyset\rangle_{\mathsf{f}} &= \bigcap\{\, P \subseteq R \mid P \leq_{\mathsf{f}} R \,\}\end{aligned}$$

(1.55) Proposition: (viz. 730)
Consider a ring $(R, +, \cdot)$ and a non-empty subset $\emptyset \neq X \subseteq R$. Then we can give an explicit description of the (left)-ideal generated by X. It turns out, these are given to be

$$\langle X\rangle_{\mathsf{m}} = \left\{ \sum_{i=1}^{n} a_i x_i \;\middle|\; 1 \leq n \in \mathbb{N},\ x_i \in X,\ a_i \in R \right\}$$

$$\langle X\rangle_{\mathsf{i}} = \left\{ \sum_{i=1}^{n} a_i x_i b_i \;\middle|\; 1 \leq n \in \mathbb{N},\ x_i \in X,\ a_i, b_i \in R \right\}$$

Suppose R is any semi-ring and denote $\pm X := \{\, x \mid x \in X \,\} \cup \{\, -x \mid x \in X \,\}$ then we can also give an explicit description of the sub-semiring of R generated by X (and if R is a ring also of the sub-ring of R generated by X), which are given to be

$$\langle X\rangle_{\mathsf{s}} = \left\{ \sum_{i=1}^{m} \prod_{j=1}^{n} x_{i,j} \;\middle|\; 1 \leq m, n \in \mathbb{N},\ x_{i,j} \in \pm X \right\}$$

$$\langle X\rangle_{\mathsf{r}} = \langle X \cup \{\, 1 \,\}\rangle_{\mathsf{s}}$$

Finally suppose that R even is a field, referring to the generated sub-ring we can also give an explicit description of the sub-field of R generated by X

$$\langle X\rangle_{\mathsf{f}} = \left\{ ab^{-1} \mid a, b \in \langle X\rangle_{\mathsf{r}},\ b \neq 0 \right\}$$

Ideals have been introduced into the thoery of rings, as computations with ordinary elements of rings may have very strange results. Thus instead of looking at $a \in R$ one may turn to $aR \trianglelefteq_{\mathsf{i}} R$ (in a commutative ring). It turns out that it is possible to define the sum and product of ideals, as well and that this even has nicer properties than the ordinary sum and product of elements. Hence the name - aR is an *ideal* element of R. Nowadays ideals have become an indispensable tool in ring theory, mainly because they will turn out to be kernels of ring-homomorphisms. Let us turn our attention to computations with ideals:

(1.56) Proposition: (viz. 731)
Consider any semi-ring $(R,+,\cdot)$ and arbitrary ideals $\mathfrak{a}$, $\mathfrak{b}$ and $\mathfrak{c} \trianglelefteq_{\mathrm{i}} R$. Then we can use these to introduce the following subsets of R, which will always be ideals of R again

$$\begin{aligned} \mathfrak{a} \cap \mathfrak{b} &= \{\, a \in R \mid a \in \mathfrak{a} \text{ and } a \in \mathfrak{b} \,\} \\ \mathfrak{a} + \mathfrak{b} &:= \{\, a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b} \,\} \\ \mathfrak{a}\,\mathfrak{b} &:= \left\{ \sum_{i=1}^{n} a_i b_i \;\middle|\; 1 \leq n \in \mathbb{N},\, a_i \in \mathfrak{a},\, b_i \in \mathfrak{b} \right\} \end{aligned}$$

Note however that $\mathfrak{a} \cup \mathfrak{b}$ need *not* be an ideal of R (it will generate the ideal $\mathfrak{a} + \mathfrak{b}$, see below). And thereby we have the following chain of inclusions of subsets of R

$$\mathfrak{a}\,\mathfrak{b} \;\subseteq\; \mathfrak{a} \cap \mathfrak{b} \;\subseteq\; \mathfrak{a} \cup \mathfrak{b} \;\subseteq\; \mathfrak{a} + \mathfrak{b}$$

(1.57) Proposition: (viz. 731)
Let $(R,+,\cdot)$ be any semi-ring, then the compositions $\cap$, $+$ and $\cdot$ of ideals are associative, that is if $\mathfrak{a}$, $\mathfrak{b}$ and $\mathfrak{c} \trianglelefteq_{\mathrm{i}} R$ are ideals of R, then we get

$$\begin{aligned} (\mathfrak{a} \cap \mathfrak{b}) \cap \mathfrak{c} &= \mathfrak{a} \cap (\mathfrak{b} \cap \mathfrak{c}) \\ (\mathfrak{a} + \mathfrak{b}) + \mathfrak{c} &= \mathfrak{a} + (\mathfrak{b} + \mathfrak{c}) \\ (\mathfrak{a}\,\mathfrak{b})\,\mathfrak{c} &= \mathfrak{a}\,(\mathfrak{b}\,\mathfrak{c}) \end{aligned}$$

Further $\cap$ and $+$ are commutative, and if R is commutative then so is the multiplication $\cdot$ of ideals, formally again (with $\mathfrak{a}$ and $\mathfrak{b} \trianglelefteq_{\mathrm{i}} R$ again) we get the identities of

$$\begin{aligned} \mathfrak{a} \cap \mathfrak{b} &= \mathfrak{b} \cap \mathfrak{a} \\ \mathfrak{a} + \mathfrak{b} &= \mathfrak{b} + \mathfrak{a} \\ \mathfrak{a}\,\mathfrak{b} &= \mathfrak{b}\,\mathfrak{a} \end{aligned}$$

Recall that the last equality need not hold true, unless R is commutative! Addition $+$ and multiplication $\cdot$ of ideals even satisfy the distributivity laws, that is for any ideals $\mathfrak{a}$, $\mathfrak{b}$ and $\mathfrak{c} \trianglelefteq_{\mathrm{i}} R$ we also get

$$\begin{aligned} \mathfrak{a}\,(\mathfrak{b} + \mathfrak{c}) &= (\mathfrak{a}\,\mathfrak{b}) + (\mathfrak{a}\,\mathfrak{c}) \\ (\mathfrak{a} + \mathfrak{b})\,\mathfrak{c} &= (\mathfrak{a}\,\mathfrak{c}) + (\mathfrak{b}\,\mathfrak{c}) \end{aligned}$$

(1.58) Remark:
It is clear that for any ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ we get $\mathfrak{a} \cap R = \mathfrak{a}$. Thus $(\mathrm{Ideal}(R), \cap)$ is a commutative monoid with neutral element R. Likewise we get $\mathfrak{a} + 0 = \mathfrak{a}$ for any ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ and hence $(\mathrm{Ideal}(R), +)$ is a commutative monoid with neutral element 0. Finally $\mathfrak{a}\,R = \mathfrak{a} = R\,\mathfrak{a}$ for any ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ and hence $(\mathrm{Ideal}(R), \cdot)$ is a monoid with neutral element R, as well. And if R is commutative, so is $(\mathrm{Ideal}(R), \cdot)$. In this sense it is understood that $\mathfrak{a}^0 := R$ and $\mathfrak{a}^i := \mathfrak{a} \ldots \mathfrak{a}$ (i-times) for $1 \leq i \in \mathbb{N}$.

(1.59) Proposition: (viz. 731)
Now consider a ring $(R,+,\cdot)$ and two arbitrary subsets X and $Y \subseteq R$. Let $\mathfrak{a} = \langle X \rangle_{\mathfrak{i}}$ and $\mathfrak{b} = \langle Y \rangle_{\mathfrak{i}}$ be the ideals generated by these. Then the sum $\mathfrak{a}+\mathfrak{b}$ is generated by the union $X \cup Y$, formally that is

$$\mathfrak{a}+\mathfrak{b} \;=\; \langle X \cup Y \rangle_{\mathfrak{i}}$$

And if R is commutative, then the product $\mathfrak{a}\,\mathfrak{b}$ is generated by the point-wise product XY of these sets, that is $XY := \{\, xy \mid x \in X, y \in Y \,\}$ and thereby we get

$$\mathfrak{a}\,\mathfrak{b} \;=\; \langle XY \rangle_{\mathfrak{i}}$$

(1.60) Remark: (viz. 732)

(i) Due to (1.59) it often makes sense to regard sums $\mathfrak{a}+\mathfrak{b}$ or products $\mathfrak{a}\,\mathfrak{b}$ of ideals. And in (1.66) we will also the notion $\mathfrak{b}/\mathfrak{a}$ of a quotient of ideals. Thus one might also be led to think that there should be something like a *difference* of ideals. A good candidate would be the following: Consider the ideals $\mathfrak{a} \subseteq \mathfrak{b} \trianglelefteq_{\mathfrak{i}} R$ in some semi-ring $(R,+,\cdot)$. Then we might take $\langle \mathfrak{b} \setminus \mathfrak{a} \rangle_{\mathfrak{i}}$ to be the difference of $\mathfrak{b}$ minus $\mathfrak{a}$. Yet this yields nothing new, since

$$\mathfrak{a} \subset \mathfrak{b} \quimplies \mathfrak{b} = \langle \mathfrak{b} \setminus \mathfrak{a} \rangle_{\mathfrak{i}}$$

(ii) Let $(R,+,\cdot)$ be a ring again and $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \trianglelefteq_{\mathfrak{i}} R$ be a finite family of ideals of R. Then using (1.59) and induction on n it is clear that

$$\sum_{i=1}^{n} \mathfrak{a}_i \;:=\; \left\{ \sum_{i=1}^{n} a_i \;\middle|\; a_i \in \mathfrak{a}_i \right\} \;=\; \langle \bigcup_{i=1}^{n} \mathfrak{a}_i \rangle_{\mathfrak{i}}$$

This property inspires us to define the sum of an arbitrary family ($i \in I$) of ideals $\mathfrak{a}_i \trianglelefteq_{\mathfrak{i}} R$ of R. As it is not clear what we should substitute for the finite sum of elements we instead define

$$\sum_{i \in I} \mathfrak{a}_i \;:=\; \langle \bigcup_{i \in I} \mathfrak{a}_i \rangle_{\mathfrak{i}}$$

(iii) And thereby it turns out that the *infinite* sum consists of arbitrarily large but finite sums over elements of the $\mathfrak{a}_i$, formally that is

$$\begin{aligned}
\sum_{i \in I} \mathfrak{a}_i \;&=\; \left\{ \sum_{i \in I} a_i \;\middle|\; a_i \in \mathfrak{a}_i,\ \#\{\, i \in I \mid a_i \neq 0 \,\} < \infty \right\} \\
&=\; \left\{ \sum_{i \in \Omega} a_i \;\middle|\; a_i \in \mathfrak{a}_i,\ \Omega \subseteq I,\ \#\Omega < \infty \right\} \\
&=\; \left\{ \sum_{k=1}^{n} a_k \;\middle|\; n \in \mathbb{N},\ i(k) \in I,\ a_k \in \mathfrak{a}_{i(k)} \right\}
\end{aligned}$$

(iv) Let now $\mathfrak{b} \trianglelefteq_{\mathrm{i}} R$ be another ideal of R, then the distributivity rule of (1.57) generalizes to the case of infinite sums, that is

$$\left(\sum_{i\in I}\mathfrak{a}_i\right)\mathfrak{b} \;=\; \sum_{i\in I}(\mathfrak{a}_i\mathfrak{b})$$

(1.61) Proposition: (viz. 733)
Let $(R,+,\cdot)$ be a commutative ring and consider the ideals $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{a}_1,\ldots,\mathfrak{a}_k$ and $\mathfrak{b}_1,\ldots,\mathfrak{b}_k \trianglelefteq_{\mathrm{i}} R$ of R (for some $1 \leq k \in \mathbb{N}$). Then we obtain the statements

(i) $\mathfrak{a}$ and $\mathfrak{b}$ are said to be **coprime** iff they satisfy one of the following three equivalent conditions

(a) $\mathfrak{a}+\mathfrak{b} \;=\; R$

(b) $(1+\mathfrak{a})\cap\mathfrak{b} \neq \emptyset$

(c) $\exists\, a\in\mathfrak{a},\ \exists\, b\in\mathfrak{b}$ such that $a+b=1$

(ii) Suppose that $\mathfrak{a}$ and $\mathfrak{b}$ are coprime and consider any $i, j \in \mathbb{N}$, then the powers $\mathfrak{a}^i$ and $\mathfrak{b}^j$ are coprime as well, formally that is the implication

$$\mathfrak{a}+\mathfrak{b}=R \quad\Longrightarrow\quad \mathfrak{a}^i+\mathfrak{b}^j=R$$

(iii) Suppose that for any $i \in 1\ldots k$ the ideals $\mathfrak{a}$ and $\mathfrak{b}_i$ are coprime, then the ideals $\mathfrak{a}$ and $\mathfrak{b}_1\ldots\mathfrak{b}_k$ are coprime as well, formally again this is

$$\Big(\forall\, i\in 1\ldots k : \mathfrak{a}+\mathfrak{b}_i=R\Big) \quad\Longrightarrow\quad \mathfrak{a}+(\mathfrak{b}_1\ldots\mathfrak{b}_k)=R$$

(iv) Suppose that the $\mathfrak{a}_1$ to $\mathfrak{a}_k$ are *pairwise* coprime, then the product of these ideals equals their intersection. Formally this is to say, that we have the implication

$$\Big(\forall\, i\neq j\in 1\ldots k : \mathfrak{a}_i+\mathfrak{a}_j \;=\; R\Big) \quad\Longrightarrow\quad \mathfrak{a}_1\cap\cdots\cap\mathfrak{a}_k \;=\; \mathfrak{a}_1\ldots\mathfrak{a}_k$$

(1.62) Definition: (viz. 734)
Let $(R,+,\cdot)$ be any semi-ring and $\mathfrak{a} \leq_{\mathrm{m}} R$ be a left-ideal of R, then $\mathfrak{a}$ induces an equivalence relation $\sim$ on R by virtue of: For any $a, b \in R$ we define $a \sim b$ by

$$a\sim b \quad:\Longleftrightarrow\quad a-b\in\mathfrak{a}$$

The equivalence classes under this relation are called **cosets** of $\mathfrak{a}$, and for any $b \in R$ this is given to be

$$b+\mathfrak{a} \;:=\; [b] \;=\; \{\, b+a \mid a\in\mathfrak{a}\,\}$$

(refer to (0.13) for more details on this). Finally we denote the **quotient set** R modulo $\mathfrak{a}$ to be the quotient set of R under this equivalence relation $\sim$. We denote it by

$$R\Big/_{\mathfrak{a}} \;:=\; R\Big/_{\sim} \;=\; \{\, a+\mathfrak{a} \mid a\in R\,\}$$

If $\mathfrak{a} \trianglelefteq_i R$ even is an ideal (e.g. when R is commutative) then $R/\mathfrak{a}$ can even be turned into a semi-ring $(R/\mathfrak{a}, +, \cdot)$ again under the following operations

$$\begin{aligned}(a+\mathfrak{a})+(b+\mathfrak{a}) &:= (a+b)+\mathfrak{a}\\ (a+\mathfrak{a})\cdot(b+\mathfrak{a}) &:= (a\cdot b)+\mathfrak{a}\end{aligned}$$

Thereby $(R/\mathfrak{a}, +, \cdot)$ is also called the **quotient ring** or **residue ring** of R modulo $\mathfrak{a}$. Clearly, if R is commutative, then so is $R/\mathfrak{a}$. And if R is a ring, so is $R/\mathfrak{a}$, where the unit element is given to be the coset $1+\mathfrak{a}$.

(1.63) Remark:
It is common that beginners in the field of algebra encounter problems with this notion. But on the other hand the construction of taking to the quotient ring is one of the three most important tools of algebra (the others being localizing and taking tensor products). Hence we would like to append a few remarks: We have defined $R/\mathfrak{a}$ to be the quotient set of R under the equivalence relation $a-b \in \mathfrak{a}$. And the equivalence classes have been the cosets $b+\mathfrak{a}$. Hence two cosets are equal if and only if their representatives are equivalent and formally for any $a, b \in R$ this is

$$a+\mathfrak{a} = b+\mathfrak{a} \iff a-b \in \mathfrak{a}$$

And if $\mathfrak{a} \trianglelefteq_i R$ is an ideal of R we even were able to turn this quotient set $R/\mathfrak{a}$ into a ring again, under the operations above. Now don't be confused, we sometimes also employ the point-wise sum $A+B := \{\, a+b \mid a \in A, b \in B \,\}$ and product $A \cdot B := \{\, ab \mid a \in A, b \in B \,\}$ of two subsets $A, B \subseteq R$. But this a completely different story - the operations on cosets $b+\mathfrak{a}$ have been *defined* by referring to the representatives b.

(1.64) Example: (viz. 734)
Let $1 \leq n \in \mathbb{N}$ be a positive integer and consider the ideal $n\mathbb{Z} \trianglelefteq_i \mathbb{Z}$. Then we wish to present an example of the above remark: If a and $b \in \mathbb{Z}$ are any two integers, then the following three statements are equivalent

(a) $a+n\mathbb{Z} = b+n\mathbb{Z}$

(b) $a \mod n = b \mod n$

(c) there is some $k \in \mathbb{Z}$ such that $b = a+kn$

(1.65) Remark:
Intuitively speaking the residue ring $R/\mathfrak{a}$ is the ring R where all the information contained in $\mathfrak{a}$ has been erased. Thus $R/\mathfrak{a}$ only retains the information that has been stored in R but not in $\mathfrak{a}$. Hence it is no wonder that $R/\mathfrak{a}$ is "smaller" than R ($|R/\mathfrak{a}| \leq |R|$ to be precise). However $R/\mathfrak{a}$ is *not* a sub-ring of R! Let us study some special cases to enlighten things:

- In the case $\mathfrak{a} = R$ the residue ring R/R contains precisely one element, namely $0+R$. Hence $R/R = \{\, 0+R \,\}$ is the zero-ring. This matches the intuition all information has been forgotten, what remains carries the trivial structure only.

- The other extreme case is $\mathfrak{a} = \{0\}$. In this case $\mathfrak{a}$ induces the trivial relation $a \sim b \iff a = b$. Hence the residue class of a is just $a + \{0\} = \{a\}$. Therefore we have a natural identification

$$R \longleftrightarrow R \Big/ _{\{0\}} \; : \; a \mapsto \{ a \}$$

 Again this matches the intuition: $\{0\}$ contains no information hence $R/\{0\}$ retains all the information of R. In fact we have just rewritten any $a \in R$ as $\{a\} \in R/\{0\}$.

- Now consider any commutative ring $(R, +, \cdot)$ and build the polynomial ring $R[t]$ upon it. Then the ideal $\mathfrak{a} = tR[t]$ allows us to regain R from $R[t]$. Formally there is a natural identification

$$R \longleftrightarrow R[t] \Big/ _{tR[t]} \; : \; a \mapsto at^0 + tR[t]$$

 Hence one should think that $tR[t]$ contains the information we have added by going to the polynomial ring $R[t]$. Forgetting it we return to R. Further it is nice to note that the same is true for the formal power series $R[\![t]\!]$ instead of $R[t]$. The same amount of information that has been added is lost, by taking to the quotient ring.

 Prob it is clear that $R \to R[t] : a \mapsto at^0$ is injective and for $a \neq b \in R$ we even get $at^0 - bt^0 = (a-b)t^0 \notin tR[t]$. This means that even $a \mapsto at^0 + tR[t]$ is injective. And if we are given an arbitrary polynomial $f = a_n t^n + \cdots + a_1 t + a_0 t^0$ then $f + tR[t] = a_0 t^0 + tR[t]$ which also is the surjectivity. Note that this all is immediate from the first isomorphism theorem: $R[t] \to R : f \mapsto f[0]$ has kernel $tR[t]$ and image R.

- Likewise (for any $1 \leq n \in \mathbb{N}$) we obtain a natural identification between the ring $\mathbb{Z}_n$ (as defined in (1.28)) and the residue ring $\mathbb{Z}/n\mathbb{Z}$ via the isomorphism

$$\mathbb{Z} \Big/ _{n\mathbb{Z}} \; \xrightarrow{\sim} \; : \; a + n\mathbb{Z} \; \mapsto \; a \mod n$$

 This example teaches that the properties of the residue ring (here $\mathbb{Z}/n\mathbb{Z}$) may well differ from those of the ring (here $\mathbb{Z}$). E.g. $\mathbb{Z}$ is an integral domain, whereas $\mathbb{Z}/4\mathbb{Z}$ is not $((2 + 4\mathbb{Z})(2 + 4\mathbb{Z}) = 0 + 4\mathbb{Z})$. On the other hand $\mathbb{Z}/2\mathbb{Z}$ is a field, whereas $\mathbb{Z}$ is not.

 Prob first of all $\Phi(a + n\mathbb{Z}) = a \mod n$ is well-defined and bijective, according to (1.64). The inverse map is just the canonical projection $\varrho(r) = r + n\mathbb{Z}$. For the homomorphism property of Φ let us write (by division with remainder) $a = pn + r$ and $b = qn + s$ where $r = a \mod n$ and $s = b \mod n$. Then $a + b = (p + q)n + (r + s)$ and $ab = (pqn + ps + qr)n + rs$. Hence we can compute, using (1.64) again

$$\begin{aligned} \Phi((a + n\mathbb{Z}) + (b + n\mathbb{Z})) &= (a + b) \mod n = (r + s) \mod n \\ \Phi((a + n\mathbb{Z}) \cdot (b + n\mathbb{Z})) &= (ab) \mod n = (rs) \mod n \end{aligned}$$

 But by definition of $\mathbb{Z}_n$ we have the compositions $r + s = (r + s) \mod n$ and $rs = (rs) \mod n$ hence Φ truly transfers the structure of $\mathbb{Z}/n\mathbb{Z}$ onto $\mathbb{Z}_n$. In particular $\mathbb{Z}_n$ is a commutative ring again.

(1.66) Lemma: (viz. 734)

Correspondence Theorem: Consider any semi-ring $(R,+,\cdot)$ and an ideal $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$, then we obtain a 1-to-1 correspondence between the ideals of the residue ring $R/\mathfrak{a}$ and the ideals of R containing $\mathfrak{a}$. For this correspondence let us denote $\mathfrak{b}/\mathfrak{a} := \{ b+\mathfrak{a} \mid b \in \mathfrak{b} \}$, then we get

$$\begin{array}{rcl} \text{Ideal}\left(R\big/\mathfrak{a}\right) & \longleftrightarrow & \{ \mathfrak{b} \trianglelefteq_{\mathfrak{i}} R \mid \mathfrak{a} \subseteq \mathfrak{b} \} \\ \mathfrak{u} & \mapsto & \{ b \in R \mid b+\mathfrak{a} \in \mathfrak{u} \} \\ \mathfrak{b}\big/\mathfrak{a} & \hookleftarrow & \mathfrak{b} \end{array}$$

And this correspondence even is compatible with intersections, sums and products of deals and the generation of ideals. To be precise, we get the following three additional statements

(i) Consider an arbitrary subset $X \subseteq R$ and denote $X/\mathfrak{a} := \{ x+\mathfrak{a} \mid x \in X \}$ its set of residue classes. Then the ideal generated by $X/\mathfrak{a}$ is the ideal generated by $X \cup \mathfrak{a}$ modulo $\mathfrak{a}$

$$\langle X \rangle_{\mathfrak{i}} + \mathfrak{a}\big/\mathfrak{a} \;=\; \langle X\big/\mathfrak{a} \rangle_{\mathfrak{i}}$$

(ii) Let $I \neq \emptyset$ be any non-empty index set and for any $i \in I$ let $\mathfrak{b}_i \trianglelefteq_{\mathfrak{i}} R$ be an ideal of R containing $\mathfrak{a} \subseteq \mathfrak{b}_i$. Then we get the following identities for the sums and intersections

$$\begin{aligned} \bigcap_{i\in I} \mathfrak{b}_i\big/\mathfrak{a} &= \textstyle\bigcap_{i\in I} \mathfrak{b}_i\big/\mathfrak{a} \\ \sum_{i\in I} \mathfrak{b}_i\big/\mathfrak{a} &= \textstyle\sum_{i\in I} \mathfrak{b}_i\big/\mathfrak{a} \end{aligned}$$

(iii) If $\mathfrak{b}_1, \ldots, \mathfrak{b}_n \trianglelefteq_{\mathfrak{i}} R$ are finitely many ideals of R containing $\mathfrak{a} \subseteq \mathfrak{b}_i$ (for any $i \in 1 \ldots n$), then we get the following identity for the products

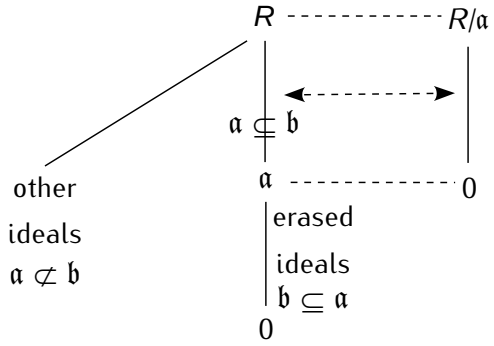
$$\prod_{i=1}^{n} \mathfrak{b}_i\big/\mathfrak{a} \;=\; \textstyle\prod_{i=1}^{n} \mathfrak{b}_i\big/\mathfrak{a}$$

(1.67) Remark:
Let $(R,+,\cdot)$ be a semi-ring and $\mathfrak{a}, \mathfrak{b} \trianglelefteq_{\mathfrak{i}} R$ be two ideals, such that $\mathfrak{a} \subseteq \mathfrak{b}$. Recall that we defined the ideal $\mathfrak{b}/\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R/\mathfrak{a}$ to be the set $\mathfrak{b}/\mathfrak{a} = \{ b+\mathfrak{a} \mid b \in \mathfrak{b} \}$. Then it is easy to see that for any $x \in R$ we even get the following equivalence

$$x \in \mathfrak{b} \iff x+\mathfrak{a} \in \mathfrak{b}\big/\mathfrak{a}$$

Prob If $x \in \mathfrak{b}$ then $x+\mathfrak{a} \in \mathfrak{b}/\mathfrak{a}$ is true by definition. And if conversely $x+\mathfrak{a} \in \mathfrak{b}/\mathfrak{a}$ then there is some $b \in \mathfrak{b}$ such that $x+\mathfrak{a} = b+\mathfrak{a}$. That is $x-b \in \mathfrak{a} \subseteq \mathfrak{b}$ and hence $x+\mathfrak{b} = b+\mathfrak{b} = 0+\mathfrak{b}$ again. But the latter already means $x \in \mathfrak{b}$.

(1.68) Remark:
The following graphic is supposed to illustrate the situation: Going from R to $R/\mathfrak{a}$ all the ideals below $\mathfrak{a}$ are deleted, while those ideals $\mathfrak{b} \trianglelefteq_{\mathfrak{i}} R$ with $\mathfrak{a} \subseteq \mathfrak{b}$ are preserved. Those ideals that were not comparable to $\mathfrak{a}$ are lost entirely, their algebraic structure defaced:



(1.69) Remark:
We will soon introduce the notion of a homomorphism, an example of such a thing is the following map that sends $b \in R$ to its equivalence class $b + \mathfrak{a}$ of $R/\mathfrak{b}$

$$\varrho \;:\; R \twoheadrightarrow R\Big/_{\mathfrak{a}} \;:\; b \mapsto b + \mathfrak{a}$$

It is clear that this mapping is surjective. And by definition the preimage of any subset $\mathfrak{u} \subseteq R/\mathfrak{a}$ is just $\varrho^{-1}(\mathfrak{u}) = \{\, b \in R \mid b + \mathfrak{a} \in \mathfrak{u} \,\}$. Finally it also is clear that for any ideal $\mathfrak{b} \trianglelefteq_{\mathrm{i}} R$ with $\mathfrak{a} \subseteq \mathfrak{b}$ the image of $\mathfrak{b}$ under ϱ is given to be

$$\varrho(\mathfrak{b}) \;=\; \{\, b + \mathfrak{a} \mid b \in \mathfrak{b} \,\} \;=\; \mathfrak{b}\Big/_{\mathfrak{a}}$$

Altogether that is: The above correspondence of ideals is just given by ϱ acting on certain subsets of R (to be precise: on the set of ideals $\mathfrak{b}$ of R that contain $\mathfrak{a}$). That is using these concepts, we could have written the correspondence theorem of ideals in terms of $\mathfrak{b} \mapsto \varrho(\mathfrak{b})$ and $\mathfrak{u} \mapsto \varrho^{-1}(\mathfrak{u})$.

(1.70) Example:
Let us give a well-known, neat little application of the theory: The usual way of denoting integers $a \in \mathbb{Z}$ is using the *decimal representation*, e.g. $273 = 2 \cdot 100 + 7 \cdot 10 + 3 \cdot 1$. Generally we write $a = a_n \ldots a_1 a_0$ iff $a_k \in 0 \ldots 9$ and

$$a \;=\; \sum_{k=0}^{n} a_k \cdot 10^k$$

As 2 divides 10 we get $a + 2\mathbb{Z} = a_0 + 2\mathbb{Z}$ and hence it is clear that 2 divides a if and only if 2 divides a_0 (the same holds true if we replace 2 by 5). We will introduce the notation $a \mid b$ for *a divides b* in (2.48). Using this already, we have just seen the equivalence, of

$$2 \mid a \quad\Longleftrightarrow\quad 2 \mid a_0$$

Also it is customary to define the *cross-sum* of a to be the sum of the digits a_k in the decimal representation of a. That is for the above a we define the map $\varphi : \mathbb{Z} \to \mathbb{Z}$ by letting

$$\phi(a) \;:=\; \sum_{k=0}^{n} a_k \;\in\; \mathbb{N}$$

E.g. the cross sum of 273 is $2+7+3=12$. Now, as $10=3\cdot 3+1$ we have $10+3\mathbb{Z}=1+3\mathbb{Z}$, and thereby $10^k+3\mathbb{Z}=(10+3\mathbb{Z})^k=(1+3\mathbb{Z})^k=1+3\mathbb{Z}$. This enables us to compute

$$\begin{aligned} a+3\mathbb{Z} &= \sum_{k=0}^{n} a_k\cdot 10^k+3\mathbb{Z} = \sum_{k=0}^{n} a_k\cdot(10^k+3\mathbb{Z}) \\ &= \sum_{k=0}^{n} a_k\cdot(1+3\mathbb{Z}) = \sum_{k=0}^{n} a_k+3\mathbb{Z} = \phi(a)+3\mathbb{Z} \end{aligned}$$

That is $a+3\mathbb{Z}=\phi(a)+3\mathbb{Z}$ and in particular we have $3 \mid a$ if and only if $\phi(a)+3\mathbb{Z}=a+3\mathbb{Z}=0+3\mathbb{Z}$ which is equivalent to $3 \mid \phi(a)$ again. That is we can check whether a is divisible by 3 just by checking whether the cross-sum $\phi(a)$ of a is divisible by 3.

$$3 \mid a \iff 3 \mid \phi(a)$$

E.g. $\phi(273)=12$ is divisible by 3 and hence 273 is divisible by 3, as well - in fact $273=3\cdot 91$. We can even iterate the cross summation, e.g. $\phi(\phi(273))=3$ which is easier to divide by 3. Also, as $10+9\mathbb{Z}=1+9\mathbb{Z}$ as well, the same reasoning holds true if we replace 3 by 9.

(1.71) Remark: $(\diamondsuit)$
Actually we have already shown some further statements in the proof of (1.66) concerning notions, that have to be introduced, yet: Let $(R,+,\cdot)$ be a commutative ring, then the above correspondence of ideals also interlocks maximal ideals, prime ideals and radical ideals, that is:

$$\begin{array}{ccc} \mathrm{Ideal}\left(R/\mathfrak{a}\right) & \longleftrightarrow & \{\,\mathfrak{b}\in \mathrm{Ideal}R \mid \mathfrak{a}\subseteq\mathfrak{b}\,\} \\ \cup & & \cup \\ \mathrm{Srad}\left(R/\mathfrak{a}\right) & \longleftrightarrow & \{\,\mathfrak{b}\in \mathrm{Srad}(R) \mid \mathfrak{a}\subseteq\mathfrak{b}\,\} \\ \cup & & \cup \\ \mathrm{Spec}\left(R/\mathfrak{a}\right) & \longleftrightarrow & \{\,\mathfrak{p}\in \mathrm{Spec}(R) \mid \mathfrak{a}\subseteq\mathfrak{p}\,\} \\ \cup & & \cup \\ \mathrm{Smax}\left(R/\mathfrak{a}\right) & \longleftrightarrow & \{\,\mathfrak{m}\in \mathrm{Smax}(R) \mid \mathfrak{a}\subseteq\mathfrak{m}\,\} \end{array}$$

That is the ideal $\mathfrak{b}\trianglelefteq_{\mathrm{i}} R$ with $\mathfrak{a}\subseteq\mathfrak{b}$ is radical if and only if the corresponding ideal $\mathfrak{b}/\mathfrak{a}\trianglelefteq_{\mathrm{i}} R/\mathfrak{a}$ is radical, too. Likewise $\mathfrak{a}\subseteq\mathfrak{b}\trianglelefteq_{\mathrm{i}} R$ is prime (maximal) iff $\mathfrak{b}/\mathfrak{a}\trianglelefteq_{\mathrm{i}} R/\mathfrak{a}$ is prime (maximal). In fact we even have the following equality of radical ideals for any $\mathfrak{b}\trianglelefteq_{\mathrm{i}} R$ with $\mathfrak{a}\subseteq\mathfrak{b}$

$$\sqrt{\mathfrak{b}/\mathfrak{a}} = \sqrt{\mathfrak{b}}/\mathfrak{a}$$

(1.72) Example: $(\diamondsuit)$
Consider the ring $(\mathbb{Z},+,\cdot)$, as $\mathbb{Z}$ is an Euclidean domain all its ideals are of the form $a\mathbb{Z}$ for some $a\in\mathbb{Z}$ (cf. to section 2.7 for a proof). We now fix some ideal $\mathfrak{a}:=a\mathbb{Z}$, then $a\mathbb{Z}\subseteq b\mathbb{Z}$ is equivalent to b dividing a (see section 2.5 for details). Hence by the correspondence theorem the ideals of $\mathbb{Z}_a=\mathbb{Z}/a\mathbb{Z}$ are

$$\mathrm{Ideal}\left(\mathbb{Z}/a\mathbb{Z}\right) = \left\{ b\mathbb{Z}/a\mathbb{Z} \;\middle|\; b \mid a \right\}$$

1.7 Homomorphisms

(1.73) Definition:
Let $(R,+,\cdot)$ and $(S,+,\cdot)$ be arbitrary semi-rings, a mapping $\varphi : R \to S$ is said to be a **homomorphism of semi-rings** (or shortly a *semi-ring-homomorphism*) iff for any $a, b \in R$ it satisfies the properties

(1) $\varphi(a+b) \;=\; \varphi(a)+\varphi(b)$

(2) $\varphi(a\cdot b) \;=\; \varphi(a)\cdot\varphi(b)$

And if R and S even are rings having the unit elements 1_R and 1_S respectively, then φ is said to be a **homomorphism of rings** (or shortly a *ring-homomorphism*) iff for any $a, b \in R$ it satisfies the properties

(1) $\varphi(a+b) \;=\; \varphi(a)+\varphi(b)$

(2) $\varphi(a\cdot b) \;=\; \varphi(a)\cdot\varphi(b)$

(3) $\varphi(1_R) \;=\; 1_S$

And we will denote the set of all semi-ring-homomorphisms, respectively of all ring-homomorphisms (as such, these are subsets of $\mathcal{F}(R,S)$), from R to S by

$$\begin{aligned} \mathrm{shom}(R,S) &:= \{\, \varphi : R \to S \mid (1) \text{ and } (2) \,\} \\ \mathrm{rhom}(R,S) &:= \{\, \varphi : R \to S \mid (1), (2) \text{ and } (3) \,\} \end{aligned}$$

And if $\varphi : R \to S$ is a homomorphism of semi-rings, then we define its **image** $\mathrm{im}(\varphi) \subseteq S$ and its **kernel** $\mathrm{kn}(\varphi) \subseteq R$ to be the following subsets, of the respective semi-rings

$$\begin{aligned} \mathrm{im}(\varphi) &:= \varphi(R) \;=\; \{\, \varphi(a) \mid a \in R \,\} \\ \mathrm{kn}(\varphi) &:= \varphi^{-1}(0_S) \;=\; \{\, a \in R \mid \varphi(a) = 0 \,\} \end{aligned}$$

(1.74) Remark:
In literature it is customary to only write $\mathrm{hom}(R,S)$ instead of what we denoted by $\mathrm{shom}(R,S)$ or $\mathrm{rhom}(R,S)$. And precisely which of these two sets is meant is determined by context only, not by notation. This ambiguity gets worse with every new algebraic structure introduced and there will be quite a lot. In this text we try to increase clarity by adding the letters "s" or "r". From a systematic point of view it might be appealing to write $\mathrm{hom}_s(R,S)$ for $\mathrm{shom}(R,S)$ (and likewise $\mathrm{hom}_r(R,S)$ for $\mathrm{rhom}(R,S)$), as we have already used these indexes with substructures. Yet we will require the position of the index later on (when it comes to modules and algebras). Hence we chose to place precisely this index in front of "hom" instead.

(1.75) Example:

- The easiest example of a homomorphism of semi-rings is the so-called *zero-homomorphism* which we denote by 0 (clearly another ambiguity) and which is given to be

$$0 \;:\; R \to S \;:\; a \mapsto 0_S$$

- Let $(S,+,\cdot)$ be any semi-ring and $R \leq_s S$ be a sub-semi-ring of S. Then the inclusion $R \subseteq S$ gives rise the the *inclusion homomorphism*

$$\iota \,:\, R \hookrightarrow S \,:\, a \mapsto a$$

 Clearly this is a homomorphism of semi-rings. And if S even is a ring and $R \leq_r S$ is a sub-ring of S, then ι is a homomorphism of rings. in the special case $R = S$ this is $\iota = \mathbb{1}_R$ the *identity map*.

- Now let $(R,+,\cdot)$ be any (semi-)ring and consider some ideal $\mathfrak{a} \trianglelefteq_i R$. Then we already have introduced the quotient (semi-)ring $R/\mathfrak{a}$ in (1.62). And this gives rise to the following homomorphism of (semi-) rings (which is called *canonical epimorphism*)

$$\varrho \,:\, R \twoheadrightarrow R\Big/_{\mathfrak{a}} \,:\, b \mapsto b + \mathfrak{a}$$

 Note that the definition of the addition and multiplication on $R/\mathfrak{a}$ are precisely the properties of ϱ being a homomorphism. And also by definition the kernel of this map precisely is $\ker(\varrho) = \mathfrak{a}$. Of course ϱ is surjective and hence its image is the entire ring $\operatorname{im}(\varrho) = R/\mathfrak{a}$.

- Consider any (semi-)ring $(R,+,\cdot)$ again and let $\mathfrak{a}$, $\mathfrak{b} \trianglelefteq_i R$ be two ideals of R such that $\mathfrak{a} \subseteq \mathfrak{b}$. Then we obtain a well-defined, surjective homomorphism of (semi-)rings by letting (further note that the kernel of this map is given to be the quotient ideal $\mathfrak{b}/\mathfrak{a}$)

$$R\Big/_{\mathfrak{a}} \twoheadrightarrow R\Big/_{\mathfrak{b}} \,:\, a + \mathfrak{a} \mapsto a + \mathfrak{b}$$

 Prob if $a + \mathfrak{a} = b + \mathfrak{a}$ then $a - b \in \mathfrak{a} \subseteq \mathfrak{b}$ whence we get $a + \mathfrak{b} = b + \mathfrak{b}$ again. This already is the well-definedness and the surjectivity and homomorphism properties are clear. Further $b + \mathfrak{b} = 0 + \mathfrak{b}$ iff $b \in \mathfrak{b}$ which again is equivalent, to $b + \mathfrak{a} \in \mathfrak{b}/\mathfrak{a}$, such that we also find $\ker(\bullet) = \mathfrak{b}/\mathfrak{a}$.

- Finally we would like to present an example of a homomorphism π of semi-rings, that is *not* a homomorphism of rings as it does not preserve the unit of R. The easiest way to achieve this is by regarding the ring $R = \mathbb{Z}^2$. Then we may take to the projection

$$\pi \,:\, \mathbb{Z}^2 \to \mathbb{Z}^2 \,:\, (a,b) \mapsto (a,0)$$

(1.76) Proposition: (viz. 736)

(i) Let $(R,+,\cdot)$ and $(S,+,\cdot)$ be semi-rings and $\varphi : R \to S$ be a homomorphism of semi-rings again. Then φ already satisfies the following properties (for any $a \in R$)

$$\begin{aligned} \varphi(0_R) &= 0_S \\ \varphi(-a) &= -\varphi(a) \end{aligned}$$

(ii) And if $(R,+,\cdot)$ and $(S,+,\cdot)$ are rings, $u \in R^*$ is an invertible element of R and $\varphi : R \to S$ is a homomorphism of rings, then $\varphi(u) \in S^*$ is an invertible element of S, too with inverse

$$\varphi(u^{-1}) = \varphi(u)^{-1}$$

(iii) Let $(R,+,\cdot)$, $(S,+,\cdot)$ and $(T,+,\cdot)$ be (semi-)rings, $\varphi : R \to S$ and $\psi : S \to T$ be homomorphisms of (semi-)rings. Then the composition ψ after φ is a homomorphism of (semi-)rings again

$$\psi\varphi \;:\; R \to S \;:\; a \mapsto \psi(\varphi(a))$$

(iv) Let $(R,+,\cdot)$ and $(S,+,\cdot)$ be (semi-)rings, $\Phi : R \to S$ be a bijective homomorphism of (semi-)rings. Then the inverse map $\Phi^{-1} : S \to R$ is a homomorphism of (semi-)rings, as well.

(v) Let $(R,+,\cdot)$ and $(S,+,\cdot)$ be (semi-)rings and $\varphi : R \to S$ be a homomorphism of (semi-)rings, then the image of φ is a sub-(semi-)ring of S and its kernel is an ideal of R

$$\begin{aligned} \mathrm{im}(\varphi) &\leq_{\mathrm{s}} S \\ \mathrm{kn}(\varphi) &\trianglelefteq_{\mathrm{i}} R \end{aligned}$$

(vi) More generally let $(R,+,\cdot)$ and $(S,+,\cdot)$ be any two (semi-)rings containing the sub-(semi-)rings $P \leq_{\mathrm{s}} R$ and $Q \leq_{\mathrm{s}} S$ respectively. If now $\varphi : R \to S$ is a homomorphism of (semi-)rings, then $\varphi(P)$ and $\varphi^{-1}(Q)$ are sub-(semi-)rings again

$$\begin{aligned} \varphi(P) &\leq_{\mathrm{s}} S \\ \varphi^{-1}(Q) &\leq_{\mathrm{s}} R \end{aligned}$$

(vii) Analogously let $(R,+,\cdot)$ and $(S,+,\cdot)$ be any two semi-rings containing the (left-)ideals $\mathfrak{a} \leq_{\mathrm{m}} R$ and $\mathfrak{b} \leq_{\mathrm{m}} S$ respectively. If now $\varphi : R \to S$ is a homomorphism of semi-rings then $\varphi^{-1}(\mathfrak{b})$ is a (left-)ideal of R again. And if φ even is surjective, then $\varphi(\mathfrak{a})$ is a (left-)ideal of R

$$\varphi^{-1}(\mathfrak{b}) \leq_{\mathrm{m}} R$$

$$\varphi \text{ surjective} \implies \varphi(\mathfrak{a}) \leq_{\mathrm{m}} R$$

(viii) Let $(R,+,\cdot)$ be a ring again and $(S,+,\cdot)$ even be a skew field. Then any non-zero homomorphism of semi-rings from R to S already is a homomorphism of rings (i.e. satisfies property (3)). Formally

$$S \text{ skew-field} \implies \mathrm{shom}(R,S) = \mathrm{rhom}(R,S) \cup \{0\}$$

(ix) Now let $(R,+,\cdot)$ be a skew-field and $(S,+,\cdot)$ be an arbitrary semi-ring, then any nonzero homomorphism $\varphi : R \to S$ of semi-rings is injective

$$R \text{ skew-field} \implies \varphi \text{ injective or } \varphi = 0$$

(1.77) Proposition: (viz. 738)
Let $(R,+,\cdot)$ be an arbitrary semi-ring and $\mathfrak{a} \trianglelefteq_i R$ be any ideal in R. Then we regard the *canonical epimorphism* from R to $R/\mathfrak{a}$, that is

$$\varrho \ : \ R \to {}^{R}\!\Big/_{\mathfrak{a}} \ : \ r \mapsto r + \mathfrak{a}$$

If now $\mathfrak{b} \trianglelefteq_i R$ is any other ideal in R then the image of $\mathfrak{b}$ under ϱ is given to be $(\mathfrak{a}+\mathfrak{b})/\mathfrak{a}$ and the preimage of this set are given to be $\mathfrak{a}+\mathfrak{b}$

$$\begin{aligned} \varrho(\mathfrak{b}) &= {}^{\mathfrak{a}+\mathfrak{b}}\!\Big/_{\mathfrak{a}} \\ \varrho^{-1}(\varrho(\mathfrak{b})) &= \mathfrak{a}+\mathfrak{b} \end{aligned}$$

(1.78) Definition:
Consider any two (semi-)rings $(R,+,\cdot)$ and $(S,+,\cdot)$ and a homomorphism $\varphi : R \to S$ of (semi-)rings. Then φ is said to be a **mono-**, **epi-** or **isomorphism** of (semi-)rings, iff it is injective, surjective or bijective respectively. And a homomorphism of the form $\varphi : R \to R$ is said to be an **endomorphism** of R. And φ is said to be an **automorphism** of R iff it is a bijective endomorphism of R. Altogether we have defined the notions

φ is called	iff φ is
monomorphism	injective
epimorphism	surjective
isomorphism	bijective
endomorphism	$R = S$
automorphism	$R = S$ and bijective

And if $(R,+,\cdot)$ is any ring, then we denote the set of all ring automorphisms on R by (note that this is a group under the composition of mappings)

$$\mathrm{raut}(R) \ := \ \{\, \Phi : R \to R \mid \Phi \text{ bijective homomorphism of rings} \,\}$$

In the case that $\Phi : R \to S$ is an isomorphism of semi-rings we will abbreviate this by writing $\Phi : R \cong_s S$. And if $\Phi : R \to S$ even is an isomorphism of rings we write $\Phi : R \cong_r S$. And thereby R and S are said to be **isomorphic** if there is an isomorphism Φ between them. And in this case we write

$$\begin{aligned} R \cong_s S \ &:\Longleftrightarrow \ \exists \Phi \ : \ \Phi : R \cong_s S \\ R \cong_r S \ &:\Longleftrightarrow \ \exists \Phi \ : \ \Phi : R \cong_r S \end{aligned}$$

(1.79) Remark:

(i) If $(R,+,\cdot)$ is any ring, the set $\mathrm{rend}(R) := \mathrm{rhom}(R,R)$ of endomorphisms of the ring R is a monoid under the composition of maps. I.e. $\mathbb{1} \in \mathrm{rend}(R)$ and if both ε and $\eta : R \to R$ are endomorphism of the ring R, then $\varepsilon\eta : R \to R : a \mapsto \varepsilon(\eta(a))$ is an endomorphism of R, as well.

(ii) If $\varepsilon \in \mathrm{rend}(R)$ is an endomorphism of R, then $\mathrm{im}(\varepsilon) = \varepsilon(R) \leq_{\mathrm{r}} R$ is a sub-ring of R. But the same is true for the *fixed ring* of ε, which is defined to be

$$\mathrm{fix}(\varepsilon) \;:=\; \{\, a \in R \mid \varepsilon(a) = a \,\} \quad \leq_{\mathrm{r}} \quad \varepsilon(R)$$

Prob As $\varepsilon(0) = 0$ and $\varepsilon(1) = 1$ by assumption we have $0, 1 \in \mathrm{fix}(\varepsilon)$. And as $\mathrm{fix}(\varepsilon) = \varepsilon(\mathrm{fix}(\varepsilon)) \subseteq \varepsilon(R) = \mathrm{im}(\varepsilon)$ is clear, this is $0, 1 \in \mathrm{im}(\varepsilon)$. Also, if $u = \varepsilon(a)$ and $v = \varepsilon(b) \in \mathrm{im}(\varepsilon)$ then $u + v = \varepsilon(a) + \varepsilon(b) = \varepsilon(a + b) \in \mathrm{im}(\varepsilon)$ and $u \cdot v = \varepsilon(a) \cdot \varepsilon(b) = \varepsilon(a \cdot b) \in \mathrm{im}(\varepsilon)$ again. Thus $\mathrm{im}(\varepsilon) \leq_{\mathrm{r}} R$ is a sub-ring of R containing $\mathrm{fix}(\varepsilon)$. Now, if $a, b \in \mathrm{fix}(\varepsilon)$ then $a + b = \varepsilon(a) + \varepsilon(b) = \varepsilon(a + b)$ and $a \cdot b = \varepsilon(a) \cot \varepsilon(b) = \varepsilon(a \cdot b)$ such that $a + b$ and $a \cdot b \in \mathrm{fix}(\varepsilon)$ again. Thus $\mathrm{fix}(\varepsilon)$ is another sub-ring of R, contained in $\mathrm{im}(\varepsilon)$.

(iii) Recall the definition of the complex numbers given in (1.35). The classical example of a ring endomorphism is the complex conjugation

$$\kappa \;:\; \mathbb{C} \to \mathbb{C} \;:\; a + ib \mapsto a - ib$$

which is an automorphism of the field $\mathbb{C}$ whose fixed ring are the reals $\mathrm{fix}(\kappa) = \mathbb{R} \subseteq \mathbb{C}$. We will later see, that κ is the only automorphism of $\mathbb{C}$ that fixes $\mathbb{R}$, apart from $\mathbb{1}$.

(iv) Another example of an endomorphism of rings $\nu : \mathbb{Z}[t] \to \mathbb{Z}[t]$ thrives on the polynomial ring $\mathbb{Z}[t]$ introduced in (1.33). We take a look at $\nu(f) := f[0]$ and see that ν neither is surjective nor injective and that the fixed ring of ν is given to be

$$\mathrm{fix}(\nu) \;=\; \mathrm{im}(\nu) \;=\; \mathbb{Z} \quad \leq_{\mathrm{r}} \quad \mathbb{Z}[t]$$

(1.80) Proposition: (viz. 738)

(i) Let $(R, +, \cdot)$ and $(S, +, \cdot)$ be semi-rings and $\varphi : R \to S$ be a homomorphism of semi-rings. Then φ is injective, iff its kernel is $0 \subseteq R$, resp. surjective iff its image is S

$$\begin{aligned} \varphi \text{ injective} &\iff \mathrm{kn}(\varphi) = \{0\} \\ \varphi \text{ surjective} &\iff \mathrm{im}(\varphi) = S \end{aligned}$$

(ii) Let $(R, +, \cdot)$ and $(S, +, \cdot)$ be (semi-)rings and $\Phi : R \to S$ be a homomorphism of (semi-)rings, then the following statements are equivalent (and in this case we already get $\alpha = \beta = \Psi = \Phi^{-1}$)

(a) Φ is bijective

(b) there is some homomorphism $\Psi : S \to R$ of (semi-)rings, such that $\Psi\Phi = \mathbb{1}_R$ and $\Phi\Psi = \mathbb{1}_S$

(c) there are arbitrary maps $\alpha : S \to R$ and $\beta : S \to R$, such that $\alpha\Phi = \mathbb{1}_R$ and $\Phi\beta = \mathbb{1}_S$

(iii) Let $(R, +, \cdot)$ and $(S, +, \cdot)$ be any two semi-rings and $\Phi : R \cong_{\mathrm{s}} S$ be an isomorphism between them. Then R is a ring if and only if S is a ring. And in this case $\Phi : R \cong_{\mathrm{r}} S$ already is an isomorphism of rings.

(iv) The relation $\cong_r$ has the properties of an equivalence relation on the class of all rings (and the same is true for $\cong_s$ on the class of all semi-rings). To be precise, for all rings $(R,+,\cdot)$, $(S,+,\cdot)$ and $(T,+,\cdot)$ we obtain the following statements

$$\mathbb{1}_R : R \cong_r R$$

$$\Phi : R \cong_r S \implies \Phi^{-1} : S \cong_r R$$

$$\Phi : R \cong_r S \text{ and } \Psi : S \cong_r T \implies \Psi\Phi : R \cong_r T$$

(1.81) Remark:
Intuitively speaking two (semi-)rings $(R,+,\cdot)$ and $(S,+,\cdot)$ are isomorphic if and only if they carry precisely the same structure. A bit lax that is the elements may differ by the names they are given but nothing more. Therefore any algebraic property satisfied by R also holds true for S and vice versa. We give a few examples of this fact below, but this is really true for *any* algebraic property. Thus from an algebraic point of view, isomorphic (semi-)rings are just two copies the same thing (just like two 1 Euro coins). And the difference between equality and isomorphy is just a set-theoretical one. We verify this intuitive view by presenting a few examples - let $(R,+,\cdot)$ and $(S,+,\cdot)$ be any two semi-rings that are isomorphic under $\Phi : R \cong_s S$. Then we get

- In the above proposition (1.80.(iii)) we have already shown R is a ring if and only if S is a ring. And in this case already Φ is an isomorphism of rings.

- R is commutative if and only if S is commutative. Prob suppose that R is commutative and consider any two elements $x, y \in S$. Then let $a := \Phi^{-1}(x)$ and $b := \Phi^{-1}(y) \in R$, then we are able to compute $xy = \Phi(a)\Phi(b) = \Phi(ab) = \Phi(ba) = \Phi(b)\Phi(a) = yx$. Hence S is commutative, too. And the converse implication follows with Φ instead of Φ^{-1}.

- R is an integral domain if and only if S is an integral domain. Prob suppose that S is an integral domain and consider any two elements $a, b \in R$. If $ab = 0$ then $0 = \Phi(0) = \Phi(ab) = \Phi(a)\Phi(b)$. But as S is an integral domain this means $\Phi(a) = 0$ or $\Phi(b) = 0$. And as Φ is injective this implies $a = 0$ or $b = 0$. Hence R is an integral domain, too. And the converse implication follows with Φ^{-1} instead of Φ.

- R is a skew-field if and only if S is a skew-field. In fact for any two rings R and S we even get the stronger correspondence

 $$\Phi(R^*) = S^*$$

 Prob if $a \in R^*$ is a unit of R then $\Phi(a^{-1}) = \Phi(a)^{-1}$ and hence $\Phi(a) \in S^*$ is a unit, too. And if conversely $x \in S^*$ is a unit of S, then let $a := \Phi^{-1}(x)$ and $b := \Phi^{-1}(x^{-1})$. Thereby $ab = \Phi^{-1}(x)\Phi^{-1}(x^{-1}) = \Phi^{-1}(xx^{-1}) = \Phi(1_S) = 1_R$ and likewise $ba = 1_R$. Hence we have $a^{-1} = b$ such that $a \in R^*$ and $x \in \Phi(R^*)$ is the image of a unit of R.

(1.82) Remark: $(\diamondsuit)$
In the chapters to come we will introduce the notion of a category (in our case this would be the collection of all semi-rings or of all rings respectively). And in any category there is the notion of *monomorphisms*, *epimorphisms* and *isomorphisms*. That is let $(R,+,\cdot)$ and $(S,+,\cdot)$ be two (semi-)rings. Then $\varphi : R \to S$ will be called a **monomorphism** in the category of (semi-)rings, iff it is a homomorphism of (semi-)rings, such that for any (semi-)ring $(Q,+,\cdot)$ and any two homomorphisms α, $\beta : Q \to R$ of (semi-)rings we would have the implication

$$\varphi\alpha = \varphi\beta \quad \Longrightarrow \quad \alpha = \beta$$

Likewise $\varphi : R \to S$ will be called a **epimorphism** in the category of (semi-) rings, iff it is a homomorphism of (semi-)rings, such that for any (semi-)ring $(T,+,\cdot)$ and any two homomorphisms α, $\beta : S \to T$ of (semi-)rings we would have the implication

$$\alpha\varphi = \beta\varphi \quad \Longrightarrow \quad \alpha = \beta$$

Finally $\Phi : R \to S$ is said to be an **isomorphism** in the category of (semi-) rings, iff it is a homomorphism of (semi-)rings and there is another homomorphism $\Psi : S \to R$ of (semi-)rings that is inverse to Φ

$$\exists\, \Psi : S \to R \;\; : \;\; \Psi\Phi = \mathbb{1}_R \text{ and } \Phi\Psi = \mathbb{1}_S$$

It is immediately clear that an injective homomorphism of (semi-)rings thereby is a monomorphism in the categorial sense. And likewise a surjective homomorphism of (semi-rings) is an epimorphism in the categorial sense. The converse implications need not be true however. Yet we have seen in the previous proposition that the two notions of isomorphy are equivalent.

(1.83) Theorem: (viz. 739) **Isomorphism Theorems**

(i) Let $(R,+,\cdot)$ and $(S,+,\cdot)$ be any two rings, $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be an ideal of R and $\varphi : R \to S$ be a homomorphism of rings. If now $\mathfrak{a} \subseteq \ker(\varphi)$ then we obtain a well-defined homomorphism of rings by virtue of the following definition

$$\widetilde{\varphi} \;:\; R\big/_{\mathfrak{a}} \to S \;:\; b + \mathfrak{a} \mapsto \varphi(a)$$

Note that in case R and S are semi-rings only and φ is a homomorphism of such, then $\widetilde{\varphi}$ still is a well-defined homomorphism of semi-rings.

(ii) **First Isomorphism Theorem**
Let $(R,+,\cdot)$ and $(S,+,\cdot)$ be any two rings and $\varphi : R \to S$ be a homomorphism of rings. Then the kernel of φ is an ideal $\ker(\varphi) \trianglelefteq_{\mathrm{i}} R$ of R and the its image $\mathrm{im}(\varphi) \leq_{\mathrm{r}} S$ is a sub-ring of S. And finally we obtain the following isomorphy of rings

$$R\big/_{\ker(\varphi)} \;\cong_{\mathrm{r}}\; \mathrm{im}(\varphi) \;:\; a + \ker(\varphi) \mapsto \varphi(a)$$

Note that in case R and S are semi-rings only and φ is a homomorphism of such, then we still get $\ker(\varphi) \trianglelefteq_{\mathrm{i}} R$, $\mathrm{im}(\varphi) \leq_{\mathrm{s}} S$ and $R/\mathfrak{a} \cong_{\mathrm{s}} \mathrm{im}(\varphi)$.

(iii) **Second Isomorphism Theorem**

Let $(S,+,\cdot)$ be a ring, $R \leq_{\mathrm{r}} S$ be a sub-ring of S and $\mathfrak{b} \trianglelefteq_{\mathrm{i}} S$ be an ideal of S. Then $\mathfrak{b} \cap R \trianglelefteq_{\mathrm{i}} R$ is an ideal of R, the set $\mathfrak{b} + R := \{\, b + a \mid b \in \mathfrak{b}, a \in R \,\} \leq_{\mathrm{r}} S$ is a sub-ring of S and $\mathfrak{b} \trianglelefteq_{\mathrm{i}} \mathfrak{b} + R$ is an ideal of $\mathfrak{b} + R$. And thereby we obtain the following isomorphy of rings

$$R \Big/ \mathfrak{b} \cap R \;\cong_{\mathrm{r}}\; \mathfrak{b} + R \Big/ \mathfrak{b} \;:\; a + \mathfrak{b} \cap R \mapsto a + \mathfrak{b}$$

Note that in case S is a semi-ring and $R \leq_{\mathrm{s}} S$ is a sub-semi-ring of S, then still $\mathfrak{b} + R \leq_{\mathrm{s}} S$, $\mathfrak{b} \trianglelefteq_{\mathrm{i}} \mathfrak{b} + R$ and we retain the isomorphy $R/\mathfrak{b} \cap R \cong_{\mathrm{s}} \mathfrak{b} + R/\mathfrak{b}$.

(iv) **Third Isomorphism Theorem**

Let $(R,+,\cdot)$ be any ring containing the ideals $\mathfrak{a} \subseteq \mathfrak{b} \trianglelefteq_{\mathrm{i}} R$, then $\mathfrak{b}/\mathfrak{a} := \{\, b + \mathfrak{a} \mid b \in \mathfrak{b} \,\} \trianglelefteq_{\mathrm{i}} R/\mathfrak{a}$ is an ideal of the quotient ring $R/\mathfrak{a}$ and we obtain the following isomorphy of rings

$$R/\mathfrak{a} \Big/ \mathfrak{b}/\mathfrak{a} \;\cong_{\mathrm{r}}\; R \Big/ \mathfrak{b} \;:\; (a + \mathfrak{a}) + \mathfrak{b} \Big/ \mathfrak{a} \mapsto a + \mathfrak{b}$$

Note in case R is a semi-ring then everything remains the same, except that the above isomorphy is an isomorphy of semi-rings (and not necessarily of rings).

1.8 Ordered Rings

In this section we will regard commutative rings that are subjected to a (as we call it) *positive* order. However it is completely independent of the other sections within this book. Its results will neither be used nor continued elsewhere. But as it is a nice generalization of the classical examples of rings – foremost $\mathbb{Z}$, as these carry a natural order – we chose to include it nevertheless. Enjoy.

(1.84) Definition:
Let $(R, +, \cdot)$ be a commutative ring, then a subset $C \subseteq R$ is said to be a **positive cone** in R, iff it satisfies the following three properties

(C1) $0, 1 \in C$

(C2) $a, b \in C \implies a + b \in C$

(C3) $a, b \in C \implies a \cdot b \in C$

Let us denote $-C := \{ -a \mid a \in C \} \subseteq R$, then a positive cone $C \subseteq R$ is said to be **proper** iff it also satisfies the following fourth property

(CP) $C \cap (-C) = \{0\}$

And a positive cone $C \subseteq R$ is said to be **total** iff it satisfies another property

(CT) $C \cup (-C) = R$

(1.85) Proposition: (viz. 740)

(i) Let $(R, +, \cdot)$ be a commutative ring and (C_i) be a family ($i \in I$) of positive cones $C_i \subseteq R$ of R, then their intersection is a positive cone in R again

$$\bigcap_{i \in I} C_i \subseteq R \text{ is a positive cone}$$

(ii) Due to (i) we may define the positive cone **generated** by any subset $A \subseteq R$ to be the smallest positive cone containing A, that is

$$\operatorname{cone}(A) := \bigcap \{ C \subseteq R \mid A \subseteq C, C \text{is a positive cone} \}$$

(iii) Let both $(R, +, \cdot)$ and $(S, +, \cdot)$ be commutative rings and $\varphi : R \to S$ be a ring homomorphism, then we get the following implications:

$$\begin{aligned} C \subseteq R \text{ positive cone} &\implies \varphi(C) \subseteq S \text{ positive cone} \\ D \subseteq S \text{ positive cone} &\implies \varphi^{-1}(D) \subseteq R \text{ positive cone} \end{aligned}$$

(1.86) Example: (viz. 740)

(i) For any commutative ring $(R,+,\cdot)$ the whole set $R \subseteq R$ is a cone in R. In fact any sub-ring $S \subseteq R$ is a cone in R. The difference between these two notions is that a sub-ring S has to be a subgroup of the additive group $(R,+)$ of the ring, whereas a positive cone $C \subseteq R$ only is s submonoid of $(R,+)$. In fact sub-rings yield rather uninteresting positive cones.

(ii) For any commutative ring $(R,+,\cdot)$ and any $1 \leq k \in \mathbb{N}$ we can interpret k as an element of R as $k_R := 1_R + \cdots + 1_R$ (k-times) and likewise for negative numbers: $(-k)_R := -(k_R)$. Then we can regard the ring homomorphism $\zeta : \mathbb{Z} \to R : k \mapsto k_R$. The image of $\mathbb{N}$ under this homomorphism is a positive cone in R

$$P \;:=\; \{\, k_R \mid k \in \mathbb{N} \,\}$$

In fact P is the smallest positive cone of R at all [that is $P = \mathrm{cone}(\emptyset)$] and hence also called the *prime cone* of R. The homomorphism has another interesting property: The kernel of ζ is an ideal in $\mathbb{Z}$ and hence there is an unique $c \in \mathbb{N}$ such that $\mathrm{kn}(\zeta) = c\,\mathbb{Z}$. This c is called the *characteristic* of R and denoted by

$$\textsc{char}(R) \;:=\; \min\{\, k \in \mathbb{N} \mid k_R = 0 \,\}$$

(iii) A special case of the above is $\mathbb{N} \subseteq \mathbb{Z}$, which obviously is a proper, total, positive cone. Note however that $\mathbb{N} \subseteq \mathbb{Q}$ is a proper, positive cone, that is *not* total.

(iv) Another well-known example is $\mathbb{R}^+ \subseteq \mathbb{C}$, which is another proper, positive, but not total cone.

(v) Generally let $(R,+,\cdot)$ be a commutative ring under a fixed positive order $\leq$ (see below), then we obtain a proper, positive cone by letting

$$R^+ \;:=\; \{\, a \in R \mid a \geq 0 \,\}$$

(vi) If $(R,+,\cdot)$ is any commutative ring, then we obtain a positive cone Δ on R (not necessarily proper nor total) by letting

$$\Delta \;:=\; \left\{\, a_1^2 + \cdots + a_n^2 \mid n \in \mathbb{N},\ a_k \in R \,\right\}$$

(vii) Let now $(R,+,\cdot)$ be an integral domain under a fixed positive order $\leq$ (see below) and consider the polynomial ring $R[x]$ over R. If $0 \neq f \in R[x]$ is any non-zero polynomial, then there are uniquely determined $k \leq n \in \mathbb{N}$ such that f is if the form:

$$f(x) \;=\; a_n x^n + \cdots + a_k x^k$$

with $a_n \neq 0$ and $a_k \neq 0$. Thereby a_n is called the *leading coefficient* of $f(x)$ whereas a_k is said to be the the *minor coefficient* of $f(x)$ which we denote by

$$\begin{aligned} \mathrm{lc}(f) &:= a_n \\ \mathrm{mc}(f) &:= a_k \end{aligned}$$

And particularly for $f = 0$ we let $\mathrm{lc}(0) := 0$ and $\mathrm{mc}(0) := 0$. It is well known that both of these maps are multiplicative and therefore we obtain two proper, positive cones, by letting:

$$\begin{aligned} R[x]^+ &:= \{ f \in R[x] \mid \mathrm{lc}(f) \geq 0 \} \\ R[x]^- &:= \{ f \in R[x] \mid \mathrm{mc}(f) \geq 0 \} \end{aligned}$$

Note that the order on $R[x]$ induced by the cone $R[x]^+$ is *non-archimedian* as for any $2 \leq n \in \mathbb{N}$ we get $x < 1/n$. This is not so with the cone $R[x]^-$ however.

(1.87) Definition:
Let $(R, +, \cdot)$ be a commutative ring and consider a partial order $\leq$ on R. That is $\leq$ is a subset of $R \times R$ satisfying the following three properties:

(O1) $\forall\, a \in R$ we have: $a \leq a$

(O2) $\forall\, a, b \in R$ we have: If $a \leq b$ and $b \leq c$ then $a \leq c$

(O3) $\forall\, a, b \in R$ we have: If $a \leq b$ and $b \leq a$ then $a = b$

Thereby we already used the customary notation $a \leq b$ for $(a, b) \in \leq$. And as usual we write $a < b$ to denote that $a \leq b$ but $a \neq b$. Now $\leq$ is said to be a **positive** order, iff for any a, $b \in R$ we get

(P1) $0 \leq 1$

(P2) $a \leq b \iff 0 \leq b - a$

(P3) $0 \leq a, b \implies 0 \leq a + b$

(P4) $0 \leq a, b \implies 0 \leq ab$

A partial order is said to be **total** iff it further satisfies the following property

(T) $\forall\, a \in R$ we have $a \leq b$ or $b \leq a$

As usual, in this case, we may define the *minimum* $a \wedge b$ and *maximum* $a \vee b$ of a, $b \in R$ to be $a \wedge b := a$ if $a \leq b$ and $a \wedge b := b$ if $b \leq a$. Likewise $a \vee b := b$ if $a \leq b$ and $a \vee b := a$ if $b \leq a$. And we can further define the **sign** $\mathrm{sgn}(a) \in R$ and **absolute value** $|a| \in R$ of an element $a \in R$

$$\mathrm{sgn}(a) := \begin{cases} 1 \text{ if } a > 0 \\ 0 \text{ if } a = 0 \\ -1 \text{ if } a < 0 \end{cases}$$

$$|a| := \begin{cases} a \text{ if } 0 \leq a \\ -a \text{ if } a \leq 0 \end{cases}$$

(1.88) Remark:
If $\leq$ is a positive order on the commutative ring $(R, +, \cdot)$ then it already satisfies the following, stronger properties for any a, b and $h \in R$

(P5) $a < b \iff 0 < b - a$

(P6) $a \leq 0 \iff 0 \leq -a$

(P7) $a \leq b \implies a + h \leq b + h$

(P8) $a \leq b, 0 \leq h \implies ah \leq bh$

(P9) $a \leq b, h \leq 0 \implies ah \geq bh$

Prob (P5) $a < b$ means $a \leq b$ but $a \neq b$. By property (P2) we get $0 \leq b - a$. Suppose $0 = b - a$, then $a = b$, which leaves $0 < b - a$ only. (P6) this is property (P2) applied to $b = 0$, (P7) if $a \leq b$ then $0 \leq b - a = (b + h) - (a + h)$ and hence - by (P2) again - $a + h \leq b + h$. (P8) if $a \leq b$ then $0 \leq b - a$ and as also $0 \leq h$ property (P4) yields $0 \leq (b - a)h = bh - ah$. Now by (P2) again $ah \leq bh$. If $h \leq 0$ then by (P6) we have $0 \leq -h$ and hence by (P8) $a(-h) \leq b(-h)$ and hence $-ah \leq -bh$. By adding $ah + bh$ and using (P7) this yields $bh \leq ah$.

(1.89) Proposition: (viz. 741)
Let $(R, +, \cdot)$ be a commutative ring and $\leq$ be a total, positive order on R. Then for any a, $b \in R$ we get the following statements

(i) $0 \leq |a|$

(ii) $a \leq |a|$

(iii) $|a|^2 = a^2$

(iv) $|a| = \mathrm{sgn}(a)a$

Now suppose that R even is an integral domain, then we get the additional properties for any a, $b \in R$

(v) $|ab| = |a||b|$

(vi) $|a + b| \leq |a| + |b|$

(vii) $||a| - |b|| \leq |a - b|$

(viii) $\mathrm{sgn}(ab) = \mathrm{sgn}(a)\mathrm{sgn}(b)$

(ix) if $a, b \geq 0$ then $a \leq b \iff a^2 \leq b^2$

(1.90) Remark:

(i) Due to property (P2) it suffices to designate the *positive* elements of R, that is those $a \in R$ with $0 \leq a$. This fully defines the order $\leq$. Hence we denote the set of positive elements of R by R^+

$$R^+ := \{ a \in R \mid a \geq 0 \}$$

And as we have seen in the example (1.86) above, the set R^+ is a proper positive cone of R.

(ii) If $\leq$ is a *total* positive order on the commutative ring R, then the positive cone $R^+ \subseteq R$ already contains all the squares of elements of R, that is

$$\forall\, a \in R \;\; : \;\; a^2 \in R^+$$

Prob if $a \geq 0$ then $a^2 = a \cdot a \geq 0$ is trivial by property (P4). Otherwise (as $\leq$ is total) we have $a \leq 0$ such that by (P7) we get $0 \leq -a$ and hence $0 \leq (-a)(-a) = a^2$ by (P2) again. Thus $a^2 \geq 0$ is true in any case, for any $a \in R$.

(iii) If $R \neq 0$ is a non-zero ring, that allows a positive order $\leq$, then R already is of characteristic 0, that is the following map is injective

$$\mathbb{Z} \to R \;:\; k \mapsto k\,1_R$$

Prob suppose there was some $n \in \mathbb{Z}$ such that $n1_R = 0$, even though $n \neq 0$. Then we may take $n \geq 1$ to be minimal (i.e. n generates the kernel $n\mathbb{Z} = \mathrm{kn}(k \mapsto k1_R)$). As $0_R \leq 1_R$ we find $1_R \leq 2_R$ and so on until $(n-1)_R \leq n_R$. Hence $0_R \leq 1_R \leq n_R = 0_R$, which yields $0_R = 1_R$, a contradiction to $R \neq 0$. Hence the kernel of $k \mapsto k1_R$ is zero, the map is injective.

(iv) $(\diamondsuit)$ If R is a commutative ring, $\leq$ is a positive order on R and M is an R-module, then there is the notion of a cone C in M: That is a subset $C \subseteq M$ is said to be a **cone** in M, iff

(1) $0 \in C$

(2) for all $x, y \in C$ we get $x + y \in C$

(3) for all $x \in C$ and all $a \geq 0$ we get $ax \in C$

If we consider R itself as an R-module then a positive cone $C \subseteq R$ in the ring R need not be a cone in the R-module R, however. As an example let us regard $R = \mathbb{R}$ under the usual order $\leq$, then $C = \mathbb{N} \subseteq \mathbb{R}$ is a positive cone, but not a cone (in the sense of mudules).

(1.91) Example: (viz. 742)

(i) If $(R, +, \cdot)$ is a commutative ring and $C \subseteq R$ is a proper positive cone in R, then we obtain a positive order on R by letting:

$$a \leq b \quad :\Longleftrightarrow \quad b - a \in C$$

(ii) Let $R := \mathbb{Z}^2$ be the 2-dimensional lattice under the point-wise operations, that is $(a,b) + (c,d) := (a + c, b + d)$ and $(a,b)(c,d) := (ac, bd)$. We install the following partial $\leq$ order on R. Then $\leq$ is a positive order on R even though R is *not* an integral domain.

$$(a,b) \leq (c,d) \quad :\Longleftrightarrow \quad a \leq c \text{ and } b \leq d$$

(iii) The natural order $0 < 1 < 2 < 3$ on $R = \mathbb{Z}_4$ is *not* positive, as we have $2 \leq 3$ but adding $1 \geq 0$ this turns into $2 + 1 = 3 > 0 = 3 + 1$.

(1.92) Proposition: (viz. 742)
Let $(R,+,\cdot)$ be a commutative ring, then we obtain a 1-to-1 correspondence between the proper positive cones C in R and the positive orders $\leq$ on R, by virtue of

$$\begin{array}{rcl} \{\, C \subseteq R \mid C \text{ proper positive cone} \,\} & \longleftrightarrow & \{\, \leq \subseteq R \times R \mid \leq \text{ positive order} \,\} \\ C & \mapsto & (a \leq b :\Longleftrightarrow b - a \in C) \\ R^+ = \{\, a \in R \mid a \geq 0 \,\} & \mapsfrom & \leq \end{array}$$

(1.93) Proposition: (viz. 742) ($\diamondsuit$)
Let $(R,+,\cdot)$ be a commtative ring, $\leq$ be a positive order on R and let N denote the set of positive non-zero divisors of R, that is

$$N := \{\, n \in R \mid n \geq 0 \text{ and } \forall\, a \in R : an = 0 \implies a = 0 \,\}$$

Then N is multiplicatively closed and we denote the localization of R in N by $Q := N^{-1}R$. Thereby we obtain a positive order on Q, by letting

$$\frac{a}{m} \leq \frac{b}{n} \quad :\Longleftrightarrow \quad an \leq bm$$

1.9 Products

(1.94) Definition:
Let $\emptyset \neq I$ be an arbitrary set and for any $i \in I$ let $(R_i, +, \cdot)$ be a semi-ring. Then we define the **(exterior) direct product** of the R_i to be just the cartesian product of the sets R_i

$$\prod_{i \in I} R_i \;:=\; \left\{ a : I \to \bigcup_{i \in I} R_i \;\middle|\; \forall\, i \in I : a(i) \in R_i \right\}$$

Let us abbreviate this set by ΠR for a moment. Then we may turn this set into a semi-ring $(\Pi R, +, \cdot)$ by defining the following addition $+$ and multiplication $\cdot$ for elements a and $b \in \Pi R$

$$a + b \;:\; I \to \bigcup_{i \in I} R_i \;:\; i \mapsto a(i) + b(i)$$

$$a \cdot b \;:\; I \to \bigcup_{i \in I} R_i \;:\; i \mapsto a(i) \cdot b(i)$$

Note that thereby the addition $a(i) + b(i)$ and multiplication $a(i)b(i)$ are those of R_i. Further note that it is customary to write (a_i) instead of $a \in \Pi R$, where the $a_i \in R_i$ are given to be $a_i := a(i)$. And using this notation the above definitions of $+$ and $\cdot$ in ΠR take the more elegant form

$$\begin{aligned} (a_i) + (b_i) &:= (a_i + b_i) \\ (a_i) \cdot (b_i) &:= (a_i \cdot b_i) \end{aligned}$$

For any $i \in I$ let us now denote the zero-element of the semi-ring R_i by 0_i. Then we define the **(exterior) direct sum** of the R_i to be the subset of those $a = (a_i) \in \Pi R$ for which only finitely many a_i are non-zero. In formal terms this is

$$\bigoplus_{i \in I} R_i \;:=\; \left\{ a \in \prod_{i \in I} R_i \;\middle|\; \#\{\, i \in I \mid a(i) \neq 0_i \,\} < \infty \right\}$$

Let us denote this set by ΣR for the moment, then $\Sigma R \;\leq_s\; \Pi R$ is a sub-semi-ring. In particular we will always understand ΠR and ΣR as semi-rings under these compositions, without explicitly mentioning it.

(1.95) Example:

- Probably the most important case is where only two (semi-)rings $(R, +, \cdot)$ and $(S, +, \cdot)$ are involved. In this case the direct product and direct sum coincide, to be the cartesian product

 $$R \oplus S \;=\; R \times S \;=\; \{\, (a, b) \mid a \in R,\; b \in S \,\}$$

 And if we write out the operations on $R \oplus S$ explicitly (recall that these were defined to be the point-wise operations) these simply read as (where a, $b \in R$ and r, $s \in S$)

 $$\begin{aligned} (a, r) + (b, s) &= (a + b, r + s) \\ (a, r)(b, s) &= (ab, rs) \end{aligned}$$

Thereby it is clear that the zero-element of $R \oplus S$ is given to be $0 = (0,0)$. And if both R and S are rings then the unit element of $R \oplus S$ is given to be $1 = (1,1)$. It also is clear that $R \oplus S$ is commutative iff both R and S are such. The remarks below just generalize these observations and give hints how these can be proved.

- Another familiar case is the following: Consider a (semi-)ring $(R, +, \cdot)$ and any non-empty index set $I \neq \emptyset$. In the examples of section 1.4 we have already studied the (semi-)ring

$$R^I := \prod_{i \in I} R = \{ f \mid f : I \to R \}$$

 In the previous example as well as in this definition here we have taken the point-wise operations. That is for two elements $f, g : I \to R$ we have defined the operations

$$\begin{aligned} f + g : I \to R &= i \mapsto f(i) + g(i) \\ fg : I \to R &= i \mapsto f(i) \cdot g(i) \end{aligned}$$

 And it is clear that the zero-element is given to be the constant function $0 : I \to R : i \mapsto 0$. And if R is a ring then we also have a unit element given to be the constant function $1 : I \to R : i \mapsto 1$.

- We continue with the example above. Instead of the direct product we may also take to the direct sum of R over I. That is we may regard

$$R^{\oplus I} := \bigoplus_{i \in I} R = \{ f : I \to R \mid \#\mathrm{Supp}(f) < \infty \}$$

 where $\mathrm{Supp}(f) := \{i \in I \mid f(i) \neq 0\}$. It is clear $R^{\oplus I} \subseteq R^I$ truly is a subset of the direct product. But be careful, as in any non-zero ring $R \neq 0$ we have $1 \neq 0$ we find that for infinite index sets I the unit element $1 : I \to R : i \mapsto 1$ is *not* contained in $R^{\oplus I}$. That is $R^{\oplus I}$ will not be a ring unless I is finite, even if R is such.

(1.96) Remark:
As above let $\emptyset \neq I$ be an arbitray index set and for any $i \in I$ let $(R_i, +, \cdot)$ be a (semi-)ring having the zero element 0_i (and unit element 1_i if any). Then let us denote the direct product of the R_i by ΠR and the direct sum of the R_i by ΣR. Then we would like to remark the following

- It is clear that $(\Pi R, +, \cdot)$ truly becomes a (semi-)ring under the operations above. And if we denote the zero-element of any R_i by 0_i then the zero-element of ΠR is given to be $0 = (0_i)$.

 Prob one easily checks all the properties required for a semi-ring. As an example we prove the associativity of the addition: Let $a = (a_i)$, $b = (b_i)$ and $c = (c_i) \in \Pi R$, then $((a+b)+c)_i = (a+b)_i + c_i = (a_i + b_i) + c_i = a_i + (b_i + c_i) = a_i + (b+c)_i = (a + (b+c))_i$.

- Clearly ΠR is commutative if and only if R_i is commutative for any $i \in I$. And ΠR is a ring if and only if R_i is a ring for any $i \in I$. In the latter case let us denote the unit element of R_i by 1_i. Then the unit element of ΠR is given to be $1 = (1_i)$.

Prob if all the R_i are commutative, then for any $a = (a_i)$, $b = (b_i) \in \Pi R$ we immediately see the commutativity $(ab)_i = a_i b_i = b_i a_i = (ba)_i$ of ΠR. If any R_i is a ring then for any $a = (a_i) \in \Pi R$ we get $(1a)_i = 1_i a_i = a_i$ and $(a1)_i = a_i 1_i = a_i$. And if ΠR is a ring, fix any $j \in I$ and let $a_i := 0$ for any $j \neq i \in I$. Then the same argument shows, that R_j commutative resp. is a ring.

- By definition $\Sigma R \subseteq \Pi R$ is a subset. But ΣR even is a sub-semi-ring $\Sigma R \leq_s \Pi R$ of ΠR. Yet ΣR need *not* be a sub-ring of ΠR (even if any R_i is a ring), as (1_i) need not be contained in ΣR.

 Prob consider any $a = (a_i)$ and $b = (b_i) \in \Sigma R$ and let us denote the set $S(a) := \{ i \in I \mid a_i \neq 0_i \}$. E.g. we get $S(0) = \emptyset$ and hence $0 \in \Sigma R$. Further it is clear that $S(a+b) \subseteq S(a) \cup S(b)$, $S(-a) = S(a)$ and $S(ab) \subseteq S(a) \cap S(b)$. In particular all these sets are finite again and hence $a+b$, $-a$ and $ab \in \Sigma R$, which had to be shown.

- Note that we get $\Sigma R = \Pi R$ if and only if I is a finite set. And in the case of finitely many semi-rings $R_1, \ldots, R_n$ we also use the slightly lax notation (note that thereby $R_1 \times \cdots \times R_n = R_1 \oplus \cdots \oplus R_n$)

$$\begin{aligned} R_1 \times \cdots \times R_n &:= \prod_{i=1}^{n} R_i \\ R_1 \oplus \cdots \oplus R_n &:= \bigoplus_{i=1}^{n} R_i \end{aligned}$$

- It is clear that the product of (semi-)rings is associative and commutative up to isomorphy. That is if we consider the (semi-)rings $(R, +, \cdot)$, $(S, +, \cdot)$ and $(T, +, \cdot)$, then we obtain the following isomorphies of (semi-)rings

$$\begin{aligned} R \oplus S &\cong_s S \oplus R &&: (a,b) \mapsto (b,a) \\ \big(R \oplus S\big) \oplus T &\cong_s R \oplus \big(S \oplus T\big) &&: \big((a,b),c\big) \mapsto \big(a,(b,c)\big) \end{aligned}$$

 Prob it is immediately clear that the above mappings are homomorphisms of (semi-)rings by definition of the operations on the product. And likewise it is clear (this is an elementary property of cartesian products) that these mappings also are bijective.

- Yet ΠR usually does *not* inherit any nice properties from the R_i, except being commutative or a ring. E.g. $\mathbb{Z}$ is an integral domain, but $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$ contains the zero-divisors $(1,0)$ and $(0,1)$.

- For any $j \in I$ let us denote the canonical projection from ΠR (or ΣR respectively) by π_j. Likewise let ι_j denote the canonical injection of R_j into ΠR (or ΣR respectively). That is we let

$$\pi_j : \Sigma R \twoheadrightarrow R_j : (a_i) \mapsto a_j$$

$$\iota_j : R_j \hookrightarrow \Sigma R : a_j \mapsto \left(i \mapsto \begin{cases} a_j \text{ if } i = j \\ 0_i \text{ if } i \neq j \end{cases} \right)$$

 Then it is clear that π_i and ι_j are homomorphisms of semi-rings satisfying $\pi_j \iota_j = \mathbb{1}_j$. In particular π_j is surjective and ι_j is injective. And we will often interpret R_j as a sub-semi-ring of ΠR (or ΣR respectively) by using the isomorphism $\iota_j : R_j \cong_s \operatorname{im}(\iota_j)$.

(1.97) Proposition: (viz. 743) ($\diamondsuit$)
Let $(R,+,\cdot)$ and $(S,+,\cdot)$ be any commutative rings and consider the ideals $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ and $\mathfrak{b} \trianglelefteq_{\mathrm{i}} R$. Then we obtain an ideal $\mathfrak{a} \oplus \mathfrak{b}$ of $R \oplus S$ by letting

$$\mathfrak{a} \oplus \mathfrak{b} \;:=\; \{\, (a,b) \mid a \in \mathfrak{a},\ b \in \mathfrak{b} \,\}$$

Conversely let us denote the canonical projection of $R \oplus S$ to R by $\varrho : R \oplus S \twoheadrightarrow R : (a,b) \mapsto a$ and to S by $\sigma : R \oplus S \twoheadrightarrow S : (a,b) \mapsto b$ respectively. If now $\mathfrak{u} \trianglelefteq_{\mathrm{i}} R \oplus S$ is an ideal then we get the identity

$$\mathfrak{u} \;=\; \varrho(\mathfrak{u}) \oplus \sigma(\mathfrak{u})$$

And thereby we obtain an explicit description of all ideals (respectively of all radical, prime or maximal) ideals of $R \oplus S$. These are given to be the following

$$\begin{aligned}
\mathrm{Ideal}(R \oplus S) &= \{\, \mathfrak{a} \oplus \mathfrak{b} \mid, \mathfrak{a} \in \mathrm{Ideal}(R),\ \mathfrak{b} \in \mathrm{Ideal}(S) \,\} \\
\mathrm{Srad}(R \oplus S) &= \{\, \mathfrak{a} \oplus \mathfrak{b} \mid, \mathfrak{a} \in \mathrm{Srad}(R),\ \mathfrak{b} \in \mathrm{Srad}(S) \,\} \\
\mathrm{Spec}(R \oplus S) &= \{\, \mathfrak{p} \oplus S \mid \mathfrak{p} \in \mathrm{Spec}(R) \,\} \cup \{\, R \oplus \mathfrak{q} \mid \mathfrak{q} \in \mathrm{Spec}(S) \,\} \\
\mathrm{Smax}(R \oplus S) &= \{\, \mathfrak{m} \oplus S \mid \mathfrak{m} \in \mathrm{Smax}(R) \,\} \cup \{\, R \oplus \mathfrak{n} \mid \mathfrak{n} \in \mathrm{Smax}(S) \,\}
\end{aligned}$$

(1.98) Remark: ($\diamondsuit$)
For any $i \in 1 \ldots n$ let $(R_i,+,\cdot)$ be a commutative ring and let $R := R_1 \oplus \cdots \oplus R_n$ abbreviate their direct sum. Then by induction on n we find the following pairs of equivalent statements from (1.97)

$$\begin{aligned}
\mathfrak{a} \trianglelefteq_{\mathrm{i}} R \quad &\Longleftrightarrow \quad \exists\, \mathfrak{a}_k \trianglelefteq_{\mathrm{i}} R_k \text{ (where } k \in 1 \ldots n) \;:\; \mathfrak{a} = \bigoplus_{k=1}^{n} \mathfrak{a}_k \\
\mathfrak{a} \in \mathrm{Srad}(R) \quad &\Longleftrightarrow \quad \exists\, \mathfrak{a}_k \in \mathrm{Srad}(R_k) \text{ (where } k \in 1 \ldots n) \;:\; \mathfrak{a} = \bigoplus_{k=1}^{n} \mathfrak{a}_k \\
\mathfrak{p} \in \mathrm{Spec}(R) \quad &\Longleftrightarrow \quad \exists\, m \in 1 \ldots n \;\; \exists\, \mathfrak{p}_m \in \mathrm{Spec}(R_k) \;:\; \mathfrak{p} = \bigoplus_{k=1}^{n} \begin{cases} \mathfrak{p}_m \text{ if } k = m \\ R_k \text{ if } k \neq m \end{cases} \\
\mathfrak{m} \in \mathrm{Smax}(R) \quad &\Longleftrightarrow \quad \exists\, m \in 1 \ldots n \;\; \exists\, \mathfrak{m}_m \in \mathrm{Smax}(R_k) \;:\; \mathfrak{m} = \bigoplus_{k=1}^{n} \begin{cases} \mathfrak{m}_m \text{ if } k = m \\ R_k \text{ if } k \neq m \end{cases}
\end{aligned}$$

(1.99) Theorem: (viz. 744)

(i) Consider any commutative ring $(R,+,\cdot)$ and two elements $e, f \in R$. Further let us denote the respective principal ideals by $\mathfrak{a} := eR$ and $\mathfrak{b} := fR$. If now e and f satisfy $e + f = 1$ and $ef = 0$ then we get $\mathfrak{a} + \mathfrak{b} = R$ and $\mathfrak{a} \cap \mathfrak{b} = \{0\}$, formally that is

$$e + f = 1,\ ef = 0 \quad \Longrightarrow \quad \mathfrak{a} + \mathfrak{b} = R,\ \mathfrak{a} \cap \mathfrak{b} = \{0\}$$

(ii) More generally let $(R,+,\cdot)$ be a commutative ring and $e_1,\ldots,e_n \in R$ be a collection of elements (where $n \geq 2$), such that (1) $e_1+\cdots+e_n = 1$ and (2) for any $i \neq j \in 1\ldots n$ we get $e_ie_j = 0$, then the ideals $\mathfrak{a}_i := Re_i$ satisfy the following two properties

(1) $R = \mathfrak{a}_1+\cdots+\mathfrak{a}_n$

(2) $\mathfrak{a}_1\cap\cdots\cap\mathfrak{a}_n = \{0\}$

(iii) Now let $(R,+,\cdot)$ be any (not necessarily commutative) ring and $\mathfrak{a},\ \mathfrak{b} \trianglelefteq_{\mathrm{i}} R$ be two ideals of R satisfying $\mathfrak{a}+\mathfrak{b} = R$ and $\mathfrak{a}\cap\mathfrak{b} = \{0\}$. Then we obtain the following isomorphy of rings

$$R \cong_{\mathrm{r}} R\Big/_{\mathfrak{a}} \oplus R\Big/_{\mathfrak{b}} \ :\ x \mapsto (x+\mathfrak{a}, x+\mathfrak{b})$$

(iv) **Chinese Remainder Theorem**
Let $(R,+,\cdot)$ be any commutative ring and consider finitely many ideals $\mathfrak{a}_i \trianglelefteq_{\mathrm{i}} R$ (where $i \in 1\ldots n$) of R, that are pairwise coprime. That is for any $i \neq j \in 1\ldots n$ we assume

$$\mathfrak{a}_i+\mathfrak{a}_j = R$$

Let us now denote the intersection of all the $\mathfrak{a}_i$ by $\mathfrak{a} := \mathfrak{a}_1\cap\cdots\cap\mathfrak{a}_n$. Then we obtain the following isomorphy of rings

$$R\Big/_{\mathfrak{a}} \cong_{\mathrm{r}} \bigoplus_{i=1}^{n} R\Big/_{\mathfrak{a}_i} \ :\ x+\mathfrak{a} \mapsto (x+\mathfrak{a}_1,\ldots,x+\mathfrak{a}_n)$$

(1.100) Remark:

- Combining (i) and (ii) we immediately see that, whenever we are given two elements $e,\ f \in R$ in a commutative ring R, such that $e+f = 1$ and $ef = 0$, then this induces a decomposition of R into

$$R \cong_{\mathrm{r}} R\Big/_{eR} \oplus R\Big/_{fR} \ :\ x \mapsto (x+eR, x+fR)$$

- Clearly (iii) is just a special case of the Chinese Remainder Theorem (iv). Nevertheless we gave a separate formulation (and proof) of the statement to be easily accessible. In fact (iii) talks about decomposing R into smaller rings, whereas (iv) is about solving equations:

- Suppose we are given elements $a_i \in R$ (where $i \in 1\ldots n$). Then the surjectivity of the isomorphism in (iii) guarantees that there is a solution $x \in R$ to the following system of congruences. And if x is any solution of this system, then due to the isomorphy in (iii) we also find that the set of all solutions is given to be $x+\mathfrak{a}$.

$$\begin{aligned} x+\mathfrak{a}_1 &= a_1+\mathfrak{a}_1 \\ &\vdots \\ x+\mathfrak{a}_n &= a_n+\mathfrak{a}_n \end{aligned}$$

- If $a, b \in \mathbb{Z}$ are relatively prime (this will be $1 \in \gcd\{a, b\}$) and $n := ab$, then $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$ and hence the Chinese Remainder Theorem yields the following, well-defined isomorphism of rings

$$\mathbb{Z}_n \xrightarrow{\sim} \mathbb{Z}_a \oplus \mathbb{Z}_b \ : \ k + n\mathbb{Z} \mapsto \big(k + a\mathbb{Z}, k + b\mathbb{Z}\big)$$

- However if a and $b \in \mathbb{Z}$ have a common denominator, i.e. $d \in \gcd\{a, b\}$ with $d \geq 2$ and $n := ab$ again, then $\mathbb{Z}_n$ is not isomorphic to $\mathbb{Z}_a \oplus \mathbb{Z}_b$ (not even as $\mathbb{Z}$-modules).

 Prob Let $m := ab/d$ be the least common multiple of a and b, as $d \geq 2$ we have $m < ab$. Clearly $m(k + a\mathbb{Z}, k + b\mathbb{Z}) = 0 \in \mathbb{Z}_a \oplus \mathbb{Z}_b$ as both a and b divide m. In particular $\operatorname{ord}(k + a\mathbb{Z}, k + b\mathbb{Z}) \leq m$ and therefore $\mathbb{Z}_a \oplus \mathbb{Z}_b$ has elements of order m, at most. On the other hand $1 + n\mathbb{Z} \in \mathbb{Z}_n$ has order $\operatorname{ord}(1 + n\mathbb{Z}) = n = ab > m$. That is $\mathbb{Z}_n$ has an element of higher order, than any element of $\mathbb{Z}_a \oplus \mathbb{Z}_b$. In particular $\mathbb{Z}_n$ and $\mathbb{Z}_a \oplus \mathbb{Z}_b$ can't be isomorphic (as $\mathbb{Z}$-modules).

- $(\diamondsuit)$ Let us consider an example of the above in the integers $R := \mathbb{Z}$. Let $\mathfrak{a}_1 := 8\mathbb{Z}$ and $\mathfrak{a}_2 := 15\mathbb{Z}$. As 8 and 15 are relatively prime we truly find $\mathfrak{a}_1 + \mathfrak{a}_2 = \mathbb{Z}$. And also $\mathfrak{a} = \mathfrak{a}_1 \cap \mathfrak{a}_2 = 120\mathbb{Z}$, since the least common multiple of 8 and 15 is 120. It is elementary to verify the following congruences

$$\begin{array}{rclcrcl} 105 + 8\mathbb{Z} & = & 1 + 8\mathbb{Z} & \qquad & 16 + 8\mathbb{Z} & = & 0 + 8\mathbb{Z} \\ 105 + 15\mathbb{Z} & = & 0 + 15\mathbb{Z} & & 16 + 15\mathbb{Z} & = & 1 + 15\mathbb{Z} \end{array}$$

 Hence if we are given any $a_1, a_2 \in \mathbb{Z}$ then we let $x := 105a_1 + 16a_2 \in \mathbb{Z}$ to solve the general system of congruences

$$\begin{array}{rcl} x + 8\mathbb{Z} & = & a_1 + 8\mathbb{Z} \\ x + 15\mathbb{Z} & = & a_2 + 15\mathbb{Z} \end{array}$$

Chapter 2

Commutative Rings

2.1 Maximal Ideals

Non-commutative rings can be tedious. There's quite some theory concerned with rings, that defy commutativity, especially in presence of some further assumptions, e.g. Lie algebras or Jordan algebras. But in general its hard to squeeze some general structure from non-commutative rings. Yet in the case of commutative rings, the story is quite different. These rings can display astoundingly rich structures that allow beautiful classifications. The integers are the classical example, they allow prime factorization due to division with remainder. But the same is true for polynomial rings. Here we already see that there have to be some underlying reasons for this similarity.
Historically speaking ideals have been introduced to be *ideal numbers* that have even better properties, than the numbers themselves. And the main reason why commutative rings are better behaved than non-commutative is that in the former case any ideal is contained in a maximal ideal. Translated into divisibility of numbers this means that any (non-unit) number has a prime divisor. In the non-commutative case (in modules) this is not always the case.
This seemingly insignificant property is the staging area of the vast theory with which we want to proceed. So the first task will be to introduce maximal ideals and study their basic properties. To do this we recollect and append some notions of section 0.4 in order to apply it to the case of ideals later.

(2.1) Remark: (viz. 747)

(i) Let us first recall the definition of a **partial order** on some non-empty set $X \neq \emptyset$. This is a relation $\leq$ on X [that is a subset of the form $\leq \subseteq X \times X$] such that for any x, y and $z \in X$ we get

$$\begin{aligned} x = y &\implies x \leq y \\ x \leq y,\ y \leq z &\implies x \leq z \\ x \leq y,\ y \leq x &\implies x = y \end{aligned}$$

[where we already wrote $x \leq y$ for the formal statement $(x,y) \in \leq$]. And in this case we also call $(X, \leq)$ a *partially odered set*. And in this case it is also customary to use the notation

$$x < y \quad :\Longleftrightarrow \quad x \leq y \text{ and } x \neq y$$

(ii) And $\leq$ is said to be a **linear order** on X (respectively $(X, \leq)$ is called a *linearly ordered set*), iff $\leq$ is a partial order such that any two elements of X are *comparable*, formally

$$\forall\, x, y \in X \;\; : \;\; x \leq y \text{ or } y \leq y$$

And in this case we may define the *maximum* $x \vee y$ and *minimum* of any two elements $x, y \in X$ to be the following elements of X

$$x \wedge y \;\; := \;\; \begin{cases} x \text{ if } x \leq y \\ y \text{ if } y \leq x \end{cases} \qquad x \vee y \;\; := \;\; \begin{cases} y \text{ if } x \leq y \\ x \text{ if } y \leq x \end{cases}$$

(iii) Example: If S is any set (even $S = \emptyset$ is allowed), then we may take the power set $X := \mathcal{P}(X) = \{\, A \mid A \subseteq S \,\}$ of X. Then the *inclusion relation* $\subseteq$ which is defined by

$$A \subseteq B \;\; :\Longleftrightarrow \;\; \Big(\forall\, x : x \in A \implies x \in B\Big)$$

is a partial order on S. However the inclusion $\subseteq$ almost never is a total order. E.g. regard $S := \{\, 0, 1 \,\}$. Then the elements $\{0\}$ and $\{\, 1 \,\} \in X$ of X are not comparable. In what follows we will usually consider some set $X \subseteq \mathrm{Ideal}(R) \subseteq \mathcal{P}(R)$ of ideals of a commutative ring R under the inclusion relation $\subseteq$.

(iv) Now let $(X, \leq)$ be a partially ordered set and $A \subseteq X$ be a subset. Then we define the sets A_* of *minimal* and A^* of *maximal* elements of A to be the following

$$\begin{aligned} A_* \;\; &:= \;\; \{\, a_* \in A \mid \forall\, a \in A : a \leq a_* \implies a = a_* \,\} \\ A^* \;\; &:= \;\; \{\, a^* \in A \mid \forall\, a \in A : a^* \leq a \implies a = a^* \,\} \end{aligned}$$

And an element $a_* \in A_*$ is said to be a *minimal* element of A. Likewise $a^* \in A^*$ is said to be a *maximal* element of A. Note that in general it may happen that A has several minimal (or maximal) elements or even none at all. Example: $\mathbb{N}_* = \{0\}$ and $\mathbb{N}^* = \emptyset$ under the usual order $\leq$ on $\mathbb{N}$.

(v) If $(X, \leq)$ is a linearly ordered set and $A \subseteq X$ is a subset, then maximal and minimal elements of A are uniquely determined. Formally that is

$$\begin{aligned} a, b \in A^* \quad &\implies \quad a = b \\ a, b \in A_* \quad &\implies \quad a = b \end{aligned}$$

(vi) Let again $(X, \leq)$ be a linearly ordered set and $A = \{\, a_1, \ldots, a_n \,\} \subseteq X$ be a finite subset of X. Then there is a (uniquley) determined minimal element A_* (resp. maximal element a^*) of A. And this is given to be

$$\begin{aligned} A^* &= \{\, a^* \,\} \quad \text{where} \quad a^* = \Big(\big(a_1 \vee a_2\big) \ldots\Big) \vee a_n \\ A_* &= \{\, a_* \,\} \quad \text{where} \quad a_* = \Big(\big(a_1 \wedge a_2\big) \ldots\Big) \wedge a_n \end{aligned}$$

(vii) Once again let $(X, \leq)$ be any partially ordered set and $A \subseteq X$ be a subset of X. Then it is clear that $\leq$ induces another partial order $\leq_A$ on A by restricting

$$\leq_A \ := \ (\leq) \cap (A \times A)$$

And we will write $\leq$ for $\leq_A$ again, that is we write $(A, \leq)$ instead of the more correct form $(A, \leq_A)$. Now a subset $C \subseteq X$ is said to be a **chain** in X iff $(C, \leq)$ is linearly ordered. Equivalently that is iff any two elements of C are comparable, formally

$$\forall\, x, y \in C \ : \ x \leq y \text{ or } y \leq x$$

(viii) Let us recall the **Lemma of Zorn**: Say $(X, \leq)$ is a partially ordered set (in particular $X \neq \emptyset$), such that any chain C of X has an upper bound u in X, formally

$$\forall\, C \subseteq X \ : \ C \text{ chain} \implies \exists\, u \in X\, \forall\, c \in C \ : \ c \leq u$$

Then X already contains a (not necessarily) unique maximal element - in formal terms this is

$$\exists\, x^* \in X\, \forall\, x \in X \ : \ x^* \leq x \implies x = x^*$$

Nota though it may come as a surprise the lemma of Zorn surely is the single most powerful tool in mathematics! We will see its impact on several occasions: E.g. the existence of maximal ideals or the existence of bases (in vector-spaces). We recommend taking it for granted, it is just one of the equivalent reformulations of the axiom of choice. Hence you might as well the lemma of Zorn as a set-theoretic axiom itself. In case you really want to see a proof, refer to (0.28).

(ix) In most cases we will use a quite simple form of the lemma of Zorn: Consider an arbitrary collection of sets $\mathcal{Z}$. Recall that a *chain* in $\mathcal{Z}$ is a subset $\mathcal{C} \subseteq \mathcal{Z}$ such that $\mathcal{C} \neq \emptyset$ and for any $A, B \in \mathcal{C}$ we get $A \subseteq B$ or $B \subseteq A$. Now verify that

(1) $\mathcal{Z} \neq \emptyset$ is non-empty

(2) if $\mathcal{C} \subseteq \mathcal{Z}$ is a chain, then $\bigcup \mathcal{C} \in \mathcal{Z}$ again

Then (by the lemma of Zorn, as any $C \in \mathcal{C}$ satisfies $C \subseteq \bigcup \mathcal{C}$) $\mathcal{Z}$ already contains a (not necessarily unique) $\subseteq$-maximal element $Z \in \mathcal{Z}^*$. That is for any $A \in \mathcal{Z}$ we get

$$Z \subseteq A \implies A = Z$$

(x) Of course the lemma of Zorn can also be applied to find minimal elements. In analogy to the above we obtain the following special case: Consider an arbitrary collection of sets $\mathcal{Z}$. Now verify that

(1) $\mathcal{Z} \neq \emptyset$ is non-empty

(2) if $\mathcal{C} \subseteq \mathcal{Z}$ is a chain, then $\bigcap \mathcal{C} \in \mathcal{Z}$ again

Then (by the lemma of Zorn, as any $C \in \mathcal{C}$ satisfies $\bigcap \mathcal{C} \subseteq C$) $\mathcal{Z}$ already contains a (not necessarily unique) $\subseteq$-minimal element $Z \in \mathcal{Z}_*$. That is for any $A \in \mathcal{Z}$ we get

$$A \subseteq Z \implies A = Z$$

(2.2) Definition:
Let $(R, +, \cdot)$ be a commutative ring and $\emptyset \neq \mathcal{A} \subseteq \mathrm{Ideal}(R)$ be a non-empty set of ideals of R. Then we recall the definiton of *maximal* $\mathfrak{a}^* \in \mathcal{A}^*$ and *minimal* $\mathfrak{a}_* \in \mathcal{A}_*$ elements (concerning the order "$\subseteq$") of $\mathcal{A}$:

$$\begin{aligned} \mathcal{A}^* &:= \{\, \mathfrak{a}^* \in \mathcal{A} \mid \forall\, \mathfrak{a} \in \mathcal{A} : \mathfrak{a}^* \subseteq \mathfrak{a} \implies \mathfrak{a} = \mathfrak{a}^* \,\} \\ \mathcal{A}_* &:= \{\, \mathfrak{a}_* \in \mathcal{A} \mid \forall\, \mathfrak{a} \in \mathcal{A} : \mathfrak{a} \subseteq \mathfrak{a}_* \implies \mathfrak{a} = \mathfrak{a}_* \,\} \end{aligned}$$

(2.3) Definition:
Let $(R, +, \cdot)$ be a commutative ring, then $\mathfrak{m} \subseteq R$ is said to be a **maximal ideal** of R, iff it is a maximal element of the set of all ideals but R, that is iff the following three statements hold true

(1) $\mathfrak{m}$ is an ideal: $\mathfrak{m} \trianglelefteq_{\mathrm{i}} R$

(2) $\mathfrak{m}$ is proper: $\mathfrak{m} \neq R$

(3) there is no proper ideal containing $\mathfrak{m}$, that is for any ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ we find the implication

$$\mathfrak{m} \subseteq \mathfrak{a} \implies \mathfrak{a} = \mathfrak{m} \text{ or } \mathfrak{a} = R$$

The set $\mathrm{Smax}(R)$ of all maximal ideals will be called the **maximal spectrum** of R and the intersection of all maximal ideals will be called the **Jacobson radical** of R. We denote these by

$$\begin{aligned} \mathrm{Smax}(R) &:= \Big(\mathrm{Ideal}(R) \setminus \{\, R \,\}\Big)^* \\ &= \{\, \mathfrak{m} \subseteq R \mid (1), (2) \text{ and } (3) \,\} \\ \textsc{jac}(R) &:= \bigcap \mathrm{Smax}(R) \end{aligned}$$

(2.4) Lemma: (viz. 864)

(i) Let $(R, +, \cdot)$ be a commutative ring and $\emptyset \neq \mathcal{A} \subseteq \mathrm{Ideal}(R)$ be a chain of ideals (that is for any $\mathfrak{a}$, $\mathfrak{b} \in \mathcal{A}$ we have $\mathfrak{a} \subseteq \mathfrak{b}$ or $\mathfrak{b} \subseteq \mathfrak{a}$). Then the union of all the $\mathfrak{a} \in \mathcal{A}$ is an ideal of R, formally

$$\mathcal{A} \subseteq \mathrm{Ideal}(R),\ \mathcal{A} \neq \emptyset \ \text{ is a chain } \implies \bigcup \mathcal{A} \trianglelefteq_{\mathrm{i}} R \ \text{ is an ideal}$$

(ii) Let $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be any proper (that is $\mathfrak{a} \neq R$) ideal in the commutative ring $(R, +, \cdot)$, then there is a maximal ideal of R containing $\mathfrak{a}$, formally

$$\mathfrak{a} \trianglelefteq_{\mathrm{i}} R,\ \mathfrak{a} \neq R \implies \exists\, \mathfrak{m} \in \mathrm{Smax}(R) \,:\, \mathfrak{a} \subseteq \mathfrak{m}$$

(iii) In a commutative ring $(R, +, \cdot)$ the group of units R^* of R is precisely the complement of the union of all maximal ideals of R. That is we have the identity of

$$R^* \quad = \quad R \setminus \bigcup \mathrm{Smax}(R)$$

(iv) The zero-ring is the one and only ring without maximal ideals. That is the following equivalence of

$$R = 0 \quad \Longleftrightarrow \quad \mathrm{Smax}(R) = \emptyset$$

(v) A commutative ring $(R, +, \cdot)$ is a field, iff the zero ideal $0 \trianglelefteq_{\mathrm{i}} R$ is the one and only maximal ideal of R. Formally again this is the equivalence of

$$R \text{ is a field} \quad \Longleftrightarrow \quad \mathrm{Smax}(R) = \{0\}$$

(2.5) Proposition: (viz. 878)
Let $(R, +, \cdot)$ be a commutative ring and $\mathfrak{m} \trianglelefteq_{\mathrm{i}} R$ be an ideal of R. Then the following four statements concerning $\mathfrak{m}$ are equivalent

(a) $\mathfrak{m}$ is a maximal ideal

(b) the quotient ring $R/\mathfrak{m}$ is a field

(c) the quotient ring $R/\mathfrak{m}$ is *simple* - i.e. it only contains the trivial ideals: zero and the ring itself

$$\overline{\mathfrak{a}} \trianglelefteq_{\mathrm{i}} {}^{R}\!\Big/_{\mathfrak{m}} \quad \Longrightarrow \quad \overline{\mathfrak{a}} = \{\, 0 + \mathfrak{m} \,\} \text{ or } \overline{\mathfrak{a}} = {}^{R}\!\Big/_{\mathfrak{m}}$$

(d) $\mathfrak{m}$ is coprime to any principal ideal that is not already contained in $\mathfrak{m}$, formally that is: For any $a \in R$ we get the implication

$$a \notin \mathfrak{m} \quad \Longrightarrow \quad \mathfrak{m} + aR = R$$

(2.6) Remark:
In particular the above proposition can be reformulated for the zero-ideal $\mathfrak{m} = 0$. Doing this we find the equivalence of the following three statements, for any commutative ring $(R, +, \cdot)$

(a) 0 is a maximal ideal of R

(b) R is a field

(c) R is *simple*, that is: $\mathrm{Ideal}(R) = \{0, R\}$

(2.7) Example: (viz. 819)

(i) If F is a field, then any ideal of the form $(t - a\mathbf{1})F[t]$ is a maximal ideal of the polynomial ring $F[t]$. And thereby we obtain an injective (but not generally surjective) map, by

$$F \;\hookrightarrow\; \mathrm{Smax}\big(F[t]\big) \;:\; a \;\mapsto\; (t - a\mathbf{1})F[t]$$

(ii) If $(F,+,\cdot)$ is a field, then clearly $\text{JAC}(F) = 0$, as 0 is the one and only maximal ideal of F. But this even is true for the polynomial ring $F[t]$ over F, that is we also get

$$\text{JAC}\big(F[t]\big) \;=\; 0$$

(iii) $(\diamondsuit)$ Let $n \in \mathbb{N}$ have the primary decomposition $n = p_1^{k(1)} \dots p_r^{k(r)}$. Then the residue ring $\mathbb{Z}_n$ has precisely the maximal ideals $p_i\mathbb{Z}_n$ where $i \in 1 \dots r$ and thereby the Jacobson radical of $\mathbb{Z}_n$ is

$$\text{JAC}\big(\mathbb{Z}_n\big) \;=\; (p_1 \dots p_r)\mathbb{Z}_n$$

(2.8) Proposition: (viz. 879)
Let $(R,+,\cdot)$ be any commutative ring, then we can reformulate the Jacobson radical of R: For any $j \in R$ the following two statements are equivalent

(a) $j \in \text{JAC}(R)$

(b) $\forall\, a \in R$ we get $1 - aj \in R^*$

And if $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$ is an ideal of R, then $\mathfrak{a}$ is contained in the Jacobson radical iff $1 + \mathfrak{a}$ is a subgroup of the multiplicative group. That is we obtain another equivalence of the statements

(a) $\mathfrak{a} \;\subseteq\; \text{JAC}(R)$

(b) $1 + \mathfrak{a} \;\subseteq\; R^*$

(c) $1 + \mathfrak{a} \;\leq_{\mathfrak{g}}\; R^*$

(2.9) Proposition: (viz. 880)
Let $(R,+,\cdot)$ be a commutative ring, let $\{\, \mathfrak{m}_1, \dots, \mathfrak{m}_r \,\} \subseteq \text{Smax}(R)$ be finitely many maximal ideals of R and $p, q \in \mathbb{N}$. Then we find the following properties

$$\forall\, i \neq j \in 1 \dots r \;\;:\;\; \mathfrak{m}_i^p + \mathfrak{m}_j^q = R$$

$$\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r \;=\; \mathfrak{m}_1 \dots \mathfrak{m}_r$$

$$\mathfrak{m}_1 \;\supset\; \mathfrak{m}_1\mathfrak{m}_2 \;\supset\; \dots \;\supset\; \mathfrak{m}_1\mathfrak{m}_2 \dots \mathfrak{m}_r$$

(2.10) Corollary: (viz. 883)
Let $(R,+,\cdot)$ be a commutative ring and consider $\mathfrak{m}_1, \dots, \mathfrak{m}_r \in \text{Smax}(R)$ finitely many, distinct maximal ideals of R (i.e. $\mathfrak{m}_i \neq \mathfrak{m}_j$ for any $i \neq j \in 1 \dots r$). Abbreviate their intersection by $\mathfrak{j} := \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r$ then we have the following isomorphy of rings

$$R\big/_{\mathfrak{j}} \;\cong_{\mathfrak{r}}\; \bigoplus_{i=1}^{r} R\big/_{\mathfrak{m}_i} \;:\; a + \mathfrak{j} \mapsto \Big(a + \mathfrak{m}_i\Big)$$

$$\text{Spec}\left(R\big/_{\mathfrak{j}}\right) \;=\; \text{Smax}\left(R\big/_{\mathfrak{j}}\right) \;=\; \left\{ \mathfrak{m}_i\big/_{\mathfrak{j}} \;\middle|\; i \in 1 \dots r \right\}$$

2.2 Prime Ideals

Prime ideals are another elementary concept with far-reaching consequences that can be seen as a generalization of prime numbers. In abstract algebraic geometry and number theory the set of prime ideals of a ring is the object of interest, as all many properties of the base ring reflect in there.

(2.11) Definition:
Let $(R,+,\cdot)$ be a commutative ring, then a subset $\mathfrak{p} \subseteq R$ is said to be a **prime ideal** of R, iff the following three statements hold true

(1) $\mathfrak{p}$ is an ideal: $\mathfrak{p} \trianglelefteq_{\mathfrak{i}} R$

(2) $\mathfrak{p}$ is proper $\mathfrak{p} \neq R$

(3) $\forall\, a, b \in R$ we get $ab \in \mathfrak{p} \implies a \in \mathfrak{p}$ or $b \in \mathfrak{p}$

And the set $\mathrm{Spec}(R)$ of all prime ideals of R is called (prime) **spectrum** of R. We denote it, by

$$\mathrm{Spec}(R) \;:=\; \{\, \mathfrak{p} \subseteq R \mid (1), (2) \text{ and } (3) \,\}$$

An ideal $\mathfrak{p}_* \trianglelefteq_{\mathfrak{i}} R$ is said to be a **minimal prime ideal** of R, iff it is a minimal element of $\mathrm{Spec}(R)$. That is $\mathfrak{p}_* \in \mathrm{Spec}(R)$ and for any prime ideal $\mathfrak{p} \in \mathrm{Spec}(R)$ we get the implication $\mathfrak{p} \subseteq \mathfrak{p}_* \implies \mathfrak{p} = \mathfrak{p}_*$. The set of all minimal prime ideals is called the **minimal spectrum** of R, denoted by

$$\mathrm{Smin}(R) \;:=\; \Big(\mathrm{Spec}(R)\Big)_*$$

(2.12) Proposition: (viz. 879)
Let $(R,+,\cdot)$ be a commutative ring and $\mathfrak{p} \trianglelefteq_{\mathfrak{i}} R$ be an ideal of R. Then the following four statements concerning $\mathfrak{p}$ are equivalent

(a) $\mathfrak{p}$ is a prime ideal

(b) the quotient ring $R/\mathfrak{p}$ is an integral domain (in particular non-zero)

(c) the complement $U := R \setminus \mathfrak{p}$ is a *multiplicatively closed* set, this is to say that

 (1) $1 \in U$
 (2) $u, v \in U \implies uv \in U$

(d) $\mathfrak{p} \neq R$ is a proper ideal and for any two ideals $\mathfrak{a}, \mathfrak{b} \trianglelefteq_{\mathfrak{i}} R$ we get the implication

$$\mathfrak{ab} \subseteq \mathfrak{p} \quad\Longrightarrow\quad \mathfrak{a} \subseteq \mathfrak{p} \text{ or } \mathfrak{b} \subseteq \mathfrak{p}$$

(2.13) Remark:
At this point we can reap an important harvest of the theory: *Maximal ideals are prime*. Using the machinery of algebra this can be seen in a most beautiful way: If $\mathfrak{m}$ is a maximal ideal, then $R/\mathfrak{m}$ is a field by (2.5). But fields are (by definition non-zero) integral domains. Hence $\mathfrak{m}$ already is prime by (2.12). Of course it is also possible to give a direct proof - one of these will be presented in (2.24).

(2.14) Proposition: (viz. 882)
Let $(R,+,\cdot)$ be a commutative ring and $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ be a prime ideal of R, then we find the following truisms

(i) If $a_1,\ldots,a_k \in R$ are finitely many elements then by induction we obtain the following implication

$$a_1 \ldots a_k \in \mathfrak{p} \implies \exists\, i \in 1 \ldots k \,:\, a_i \in \mathfrak{p}$$

(ii) Likewise let $\mathfrak{a}_1,\ldots,\mathfrak{a}_k \trianglelefteq_{\mathrm{i}} R$ be finitely many ideals of R, then by induction we also find the following implication

$$\bigcap_{i=1}^{k} \mathfrak{a}_i \subseteq \mathfrak{p} \implies \exists\, i \in 1 \ldots k \,:\, \mathfrak{a}_i \subseteq \mathfrak{p}$$

(iii) *Prime Avoidance*: Consider some ideals $\mathfrak{b}_1,\ldots,\mathfrak{b}_n \trianglelefteq_{\mathrm{i}} R$ where $2 \leq n \in \mathbb{N}$ such that $\mathfrak{b}_3,\ldots,\mathfrak{b}_n$ are prime ideals of R. If now $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ is any ideal, then we obtain the following implication

$$\mathfrak{a} \subseteq \bigcup_{i=1}^{n} \mathfrak{b}_i \implies \exists\, i \in 1 \ldots n \,:\, \mathfrak{a} \subseteq \mathfrak{b}_i$$

(iv) If $R \neq 0$ is a non-zero, commutative ring, then the following three statements concerning the spectrum of R are equivalent

(a) $\mathrm{Spec}(R) = \mathrm{Smax}(R)$

(b) $\mathrm{Smin}(R) = \mathrm{Smax}(R)$

(c) $(\diamondsuit)$ $\mathrm{kdim} R = 0$

(2.15) Example:
In a less formalistic way the prime avoidance lemma can be put like this: If an ideal $\mathfrak{a}$ is contained in the union of finitely many ideals $\mathfrak{b}_i$ of which at most two are non-prime, then it already is contained in one of these. In spite of the odd assumption the statement is rather sharp. In fact it may happen that $\mathfrak{a}$ is contained in the union of three strictly smaller ideals (which of course are all non-prime in this case). Let us give an example of this: Fix the field $E := \mathbb{Z}_2$ and the ideal $\mathfrak{o} := \langle s,t\rangle_{\mathrm{i}}^2 = \langle s^2, st, t^2\rangle_{\mathrm{i}} \trianglelefteq_{\mathrm{i}} E[s,t]$. Then the ring in consideration is

$$R := E[s,t] \Big/ \mathfrak{o}$$

Note that any residue class of $f \in E[s,t]$ can be represented in the form $f + \mathfrak{o} = f[0,0] + f[1,0]s + f[0,1]t + \mathfrak{o}$. That is R contains precisely 6 elements, namely $a + bs + ct + \mathfrak{o}$ where a, b and $c \in E = \mathbb{Z}_2$. Now take the following ideal

$$\begin{aligned} \mathfrak{a} &:= \langle s+\mathfrak{o}, t+\mathfrak{o}\rangle_{\mathrm{i}} \Big/ \mathfrak{o} \\ &= \{\, f+\mathfrak{o} \mid f \in E[s,t], f[0,0] = 0 \,\} \\ &= \{\, 0+\mathfrak{o}, s+\mathfrak{o}, t+\mathfrak{o}, s+t+\mathfrak{o} \,\} \end{aligned}$$

On the other hand let us also take the ideals $\mathfrak{b}_1 := (s+\mathfrak{o})R$, $\mathfrak{b}_2 := (t+\mathfrak{o})R$ and $\mathfrak{b}_2 := (s+t+\mathfrak{o})R$. Now an easy computation (e.g. for $\mathfrak{b}_1$ we get $(s+\mathfrak{o})(a+bs+ct+\mathfrak{o}) = as+\mathfrak{o}$) yields the identities

$$\begin{aligned}\mathfrak{b}_1 &= \{\,0+\mathfrak{o}, s+\mathfrak{o}\,\}\\ \mathfrak{b}_2 &= \{\,0+\mathfrak{o}, t+\mathfrak{o}\,\}\\ \mathfrak{b}_3 &= \{\,0+\mathfrak{o}, s+t+\mathfrak{o}\,\}\end{aligned}$$

And hence it is clear that any $\mathfrak{b}_i \subset \mathfrak{a}$ is a strict subset, but the union of these ideals is precisely $\mathfrak{a}$ again

$$\mathfrak{a} = \mathfrak{b}_1 \cup \mathfrak{b}_2 \cup \mathfrak{b}_3$$

(2.16) Remark: (viz. 883)
Let $(R,+,\cdot)$ be a commutative ring again and consider some ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$. Then we denote the set of all prime ideals containing $\mathfrak{a}$ by

$$\mathbb{V}(\mathfrak{a}) := \{\,\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{a} \subseteq \mathfrak{p}\,\}$$

If now $\mathfrak{a}_i \trianglelefteq_{\mathrm{i}} R$ is an ideal of R for any $i \in 1\ldots n$ resp. for any $i \in I$ (where $I \neq \emptyset$ is an arbitrary index set) and $a, b \in R$ are any elements of R, then we find the identities

$$\begin{aligned}\mathbb{V}(0) &= \operatorname{Spec}(R)\\ \mathbb{V}(R) &= \emptyset\\ \mathbb{V}\left(\sum_{i\in I}\mathfrak{a}_i\right) &= \bigcap_{i\in I}\mathbb{V}(\mathfrak{a}_i)\\ \mathbb{V}\left(\bigcap_{i=1}^{n}\mathfrak{a}_i\right) &= \bigcup_{i=1}^{n}\mathbb{V}(\mathfrak{a}_i)\\ \mathbb{V}\big(abR\big) &= \mathbb{V}\big(aR\big)\cup\mathbb{V}\big(bR\big)\end{aligned}$$

($\diamondsuit$) These simple properties have more impact than one might expect. Let us give a slight glimpse of the future, far far ahead of us: These properties state, that the sets $\mathbb{V}(\mathfrak{a})$ form the closed sets of a topology on the spectrum of R. This topology on $\operatorname{Spec}(R)$ is called the **Zariski topology** and it is the staging point of both, abstract algebraic geometry and number theory. Some more comments on this can be found in remark (2.32). These fields of mathematics deserve a textbook of their own however and we will not venture into these much further here. The following lemma however ensures however, that a ring homomorphism $\varphi : R \to S$ induces a continuous map $\operatorname{Spec}(\varphi)$ with respect to the Zariski-topology. So going to the spectrum is a contra-variant functor from the category of commutative rings to the category of topological spaces.

(2.17) Lemma: (viz. 884)
Let $(R,+,\cdot)$ and $(S,+,\cdot)$ be any two commutative rings and denote their prime spectra by $X := \operatorname{Spec}(R)$ and $Y := \operatorname{Spec}(S)$ respectively. Now consider some ring-homomorphism $\varphi : R \to S$. Then φ induces a well-defined map on the spectra of S and R, by virtue of

$$\operatorname{Spec}(\varphi) \;:\; Y \to X \;:\; \mathfrak{q} \mapsto \varphi^{-1}(\mathfrak{q})$$

For any ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ let us denote $\mathbb{V}(\mathfrak{a}) := \{\, \mathfrak{p} \in X \mid \mathfrak{a} \subseteq \mathfrak{p} \,\}$ again and for an element $a \in R$ let us appreviate $X_a := \{\, \mathfrak{p} \in X \mid a \notin \mathfrak{p} \,\}$. If now $a \in R$, $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ and $\mathfrak{b} \trianglelefteq_{\mathrm{i}} S$, then $\mathrm{Spec}(\varphi)$ satisfies

$$\begin{aligned} (\mathrm{Spec}(\varphi))^{-1}(X_a) &= Y_{\varphi(a)} \\ (\mathrm{Spec}(\varphi))\,(\mathbb{V}(\mathfrak{b})) &\subseteq \mathbb{V}\left(\varphi^{-1}(\mathfrak{b})\right) \\ (\mathrm{Spec}(\varphi))^{-1}\,(\mathbb{V}(\mathfrak{a})) &= \mathbb{V}\left(\langle \varphi(\mathfrak{a}) \rangle_{\mathrm{i}}\right) \end{aligned}$$

(2.18) Lemma: (viz. 880)

(i) Let $(R, +, \cdot)$ be a commutative ring and $\mathcal{P} \subseteq \mathrm{Spec}(R)$ be a chain of prime ideals of R (that is $\mathcal{P} \neq \emptyset$ and for any $\mathfrak{p}, \mathfrak{q} \in \mathcal{P}$ we have $\mathfrak{p} \subseteq \mathfrak{q}$ or $\mathfrak{q} \subseteq \mathfrak{p}$). Then both, the union and the intersection of all the $\mathfrak{p} \in \mathcal{P}$ are prime ideals of R again, formally

$$\mathcal{P} \subseteq \mathrm{Spec}(R),\ \mathcal{P} \neq \emptyset \quad \text{chain} \quad \Longrightarrow \quad \bigcup \mathcal{P} \text{ and } \bigcap \mathcal{P} \trianglelefteq_{\mathrm{i}} R \quad \text{prime}$$

(ii) Let $\mathcal{P} \subseteq \mathrm{Spec}(R)$ be a non-empty ($\mathcal{P} \neq \emptyset$) set of prime ideals of the commutative ring $(R, +, \cdot)$ and assume that $\mathcal{P}$ also contains any prime ideal, that is contained in any of its members

$$\forall\, \mathfrak{p} \in \mathrm{Spec}(R)\ \ \forall\, \mathfrak{q} \in \mathcal{P}\ \ :\ \ \mathfrak{p} \subseteq \mathfrak{q} \ \Longrightarrow\ \ \mathfrak{p} \in \mathcal{P}$$

then $\mathcal{P}$ already contains a minimal element: $\mathcal{P}_* \neq \emptyset$.

(iii) Let $(R, +, \cdot)$ be a commutative ring and consider an arbitrary ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ and a prime ideal $\mathfrak{q} \trianglelefteq_{\mathrm{i}} R$. We now give a short list of possible *conditions* we may impose and the respective *assumptions* that have to be supposed for $\mathfrak{a}$ and $\mathfrak{q}$ in this case

assumption	condition($\mathfrak{p}$)
$R \neq 0$	none
nothing	$\mathfrak{p} \subseteq \mathfrak{q}$
$\mathfrak{a} \neq R$	$\mathfrak{a} \subseteq \mathfrak{p}$
$\mathfrak{a} \subseteq \mathfrak{q}$	$\mathfrak{a} \subseteq \mathfrak{p} \subseteq \mathfrak{q}$

Then there is a prime ideal $\mathfrak{p}$ of R that is minimal among all prime ideals satisfying the condition imposed. Formally put: If the respective assumption is true, then

$$\{\, \mathfrak{p} \in \mathrm{Spec}(R) \mid \text{condition}(\mathfrak{p}) \,\}_* \ \neq\ \emptyset$$

(iv) Let $(R, +, \cdot)$ be a commutative ring, $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be any ideal and $\mathfrak{q} \trianglelefteq_{\mathrm{i}} R$ a prime ideal with $\mathfrak{a} \subseteq \mathfrak{q}$. Then there is a prime ideal $\mathfrak{p}_*$ minimal over $\mathfrak{a}$ that is contained in $\mathfrak{q}$. Formally that is

$$\exists\, \mathfrak{p}_* \in \{\, \mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{a} \subseteq \mathfrak{p} \,\}_* \quad \text{with} \quad \mathfrak{a} \subseteq \mathfrak{p}_* \subseteq \mathfrak{q}$$

(v) Let $(R, +, \cdot)$ be a commutative ring, $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be an ideal of R and $U \subseteq R$ be a multiplicatively closed set (that is $1 \in U$ and $u, v \in U$ implies $uv \in U$). If now $\mathfrak{a} \cap U = \emptyset$ then the set of all ideals $\mathfrak{b} \trianglelefteq_{\mathrm{i}} R$ satisfying $\mathfrak{a} \subseteq \mathfrak{b} \subseteq R \setminus U$ contains maximal elements. And any such is maximal element is a prime ideal, formally

$$\emptyset \neq \{ \mathfrak{b} \trianglelefteq_{\mathrm{i}} R \mid \mathfrak{a} \subseteq \mathfrak{b} \subseteq R \setminus U \}^* \subseteq \mathrm{Spec}(R)$$

(2.19) Corollary: (viz. 1102)

(i) Let $(R, +, \cdot)$ be a non-zero $R \neq 0$, commutative ring, then any zero-divisor of R is contained in a prime ideal that is contained in the subset of zero-divisors. In other words the set of zero-divisors of R is the union of all prime ideals of R, that are contained in the zero-divisors

$$\mathrm{zd}(R) = \bigcup \{ \mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \subseteq \mathrm{zd}(R) \}$$

(ii) In a commutative ring $(R, +, \cdot)$ the minimal prime ideals are already contained in the zero-divisors of R. Formally put, this is the following implication

$$\mathfrak{p} \in \mathrm{Smin}(R) \implies \mathfrak{p} \subseteq \mathrm{zd}(R)$$

(iii) Let $(R, +, \cdot)$ be a commutative ring and recall that we defined the *nil-radical* of R to be the ideal of nil-potent elements $\mathrm{nil}(R) := \{ a \in R \mid \exists n \in \mathbb{N} : a^n = 0 \}$. It is clear, that $\mathrm{nil}(R) \subseteq \mathfrak{p}$ for any prime ideal $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$. And thereby we find a one-to-one correspondence between the prime ideals of the rings R and $R/\mathrm{nil}(R)$

$$\mathrm{Spec}(R) \longleftrightarrow \mathrm{Spec}\left(R \Big/ \mathrm{nil}(R) \right) \; : \; \mathfrak{p} \mapsto \mathfrak{p} \Big/ \mathrm{nil}(R)$$

2.3 Radical Ideals

(2.20) Definition:
Let $(R,+,\cdot)$ be a commutative ring, $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be an ideal and $b \in R$ be an element of R. Then we define both the **radical** $\sqrt{\mathfrak{a}}$ and **fraction** $\mathfrak{a} : b$ of $\mathfrak{a}$ to be the following sets

$$\begin{aligned} \sqrt{\mathfrak{a}} &:= \left\{ a \in R \mid \exists k \in \mathbb{N} : a^k \in \mathfrak{a} \right\} \\ \mathfrak{a} : b &:= \{ a \in R \mid ab \in \mathfrak{a} \} \end{aligned}$$

Now $\mathfrak{a}$ is said to be a **radical ideal** (sometimes this is also called *perfect ideal* in literature), iff $\mathfrak{a}$ equals its own radical, that is iff we have the properties

(1) $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$

(2) $\mathfrak{a} = \sqrt{\mathfrak{a}}$

And we define the **radical spectrum** $\mathrm{Srad}(R)$ of R to be the set of all radical ideals of R, formally that is

$$\mathrm{Srad}(R) := \left\{ \mathfrak{a} \trianglelefteq_{\mathrm{i}} R \mid \mathfrak{a} = \sqrt{\mathfrak{a}} \right\}$$

(2.21) Example:
Consider the integers $\mathbb{Z}$ and some ideal $a\mathbb{Z} \trianglelefteq_{\mathrm{i}} \mathbb{Z}$ within, where we take $a \geq 2$. If we now pick up a prime factorization of a, say $a = p_1^{k(1)} \dots p_r^{k(r)}$ with pairwise distinct prime factors $p_i \neq p_j$ (whenever $i \neq j \in 1 \dots r$), then the radical ideal of $a\mathbb{Z}$ is just

$$\sqrt{a\mathbb{Z}} = (p_1 \dots p_r)\mathbb{Z}$$

Prob Let $q = p_1 \dots p_r$ and $k = \max\{ k(1), \dots, k(r) \}$. Then it is clear that $a \mid q^k$ and hence q is contained in the radical of $a\mathbb{Z}$. Conversely consider any $b \in \sqrt{a\mathbb{Z}}$, that is $a \mid b^k$ for some $k \in \mathbb{N}$. Then for any $i \in 1 \dots r$ we have $p_i \mid a \mid b^k$ such that $p_i \mid b^k$. But as p_i is prime, this yields $p_i \mid b$, but as this is true for any p_i we conclude $q \mid b$ from this.

(2.22) Proposition: (viz. 884)
Let again $(R,+,\cdot)$ be a commutative ring, $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be an ideal and $b \in R$ be an element of R. Then we obtain the following statements

(i) The fraction $\mathfrak{a} : b$ is an ideal of R again containing $\mathfrak{a}$, that is: $\mathfrak{a} \subseteq \mathfrak{a} : b \trianglelefteq_{\mathrm{i}} R$.

(ii) The radical $\sqrt{\mathfrak{a}}$ even is a radical ideal of R containing $\mathfrak{a}$, that is: $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}} \in \mathrm{Srad}(R)$.

(iii) Going to fractions resp. taking to radical ideals is monotonous, concerning the inclusion of sets. That is, if $\mathfrak{a}, \mathfrak{b} \trianglelefteq_{\mathrm{i}} R$ are any ideals and $b \in R$, then we find

$$\begin{aligned} \mathfrak{a} \subseteq \mathfrak{b} &\implies \mathfrak{a} : b \subseteq \mathfrak{b} : b \\ \mathfrak{a} \subseteq \mathfrak{b} &\implies \sqrt{\mathfrak{a}} \subseteq \sqrt{\mathfrak{b}} \end{aligned}$$

(iv) The fraction ideal $\mathfrak{a} : b$ is proper if and only if $b \notin \mathfrak{a}$, that is we find the equivalence of

$$\mathfrak{a} : b \;=\; R \quad\Longleftrightarrow\quad b \;\in\; \mathfrak{a}$$

In particular, if $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ even is a prime ideal then we are left with precisely two cases

$$\mathfrak{p} : b \;=\; \begin{cases} R \text{ if } b \in \mathfrak{p} \\ \mathfrak{p} \text{ if } b \notin \mathfrak{p} \end{cases}$$

(v) The intersection of a non-empty collection $\mathcal{A} \subseteq \operatorname{Srad}(R)$ of radical ideals is a radical ideal again

$$\mathcal{A} \subseteq \operatorname{Srad}(R),\ \mathcal{A} \neq \emptyset \quad\Longrightarrow\quad \bigcap \mathcal{A} \in \operatorname{Srad}(R)$$

(vi) Let $\mathfrak{a}_i \trianglelefteq_{\mathrm{i}} R$ be an arbitrary family of ideals ($i \in I \neq \emptyset$) and $b \in R$. Then we find the identity of

$$\bigcap_{i \in I} (\mathfrak{a}_i : b) \;=\; \left(\bigcap_{i \in I} \mathfrak{a}_i \right) : b$$

(2.23) Proposition: (viz. 885)
Let $(R, +, \cdot)$ be a commutative ring and $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be an ideal of R. Then the following four statements concerning $\mathfrak{a}$ are equivalent

(a) $\sqrt{\mathfrak{a}} \subseteq \mathfrak{a}$

(b) $\mathfrak{a} = \sqrt{\mathfrak{a}}$ is a radical ideal

(c) $\forall\, a \in R$ we get $\exists\, k \in \mathbb{N} : a^k \in \mathfrak{a} \implies a \in \mathfrak{a}$

(d) the quotient ring $R/\mathfrak{a}$ is *reduced*, i.e. it contains no non-zero nilpotents

$$\operatorname{NIL}\left(R \Big/ \mathfrak{a} \right) \;=\; \{\, 0 + \mathfrak{a} \,\}$$

(2.24) Corollary: (viz. 886)
Let $(R, +, \cdot)$ be a commutative ring and $\mathfrak{m}$, $\mathfrak{p}$ and $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be ideals of R respectively. Then we have gained the following table of equivalences

$$\begin{aligned} \mathfrak{m} \text{ maximal} &\iff R \Big/ \mathfrak{m} \text{ field} \\ \mathfrak{p} \text{ prime} &\iff R \Big/ \mathfrak{p} \text{ integral domain} \\ \mathfrak{a} \text{ radical} &\iff R \Big/ \mathfrak{a} \text{ reduced} \end{aligned}$$

where a ring S is said to be *reduced*, iff $s^k = 0$ (for some $s \in S$ and $k \in \mathbb{N}$) implies $s = 0$. And subsuming the properties of the respective quotient rings, we thereby find the inclusions

$$\operatorname{Smax}(R) \;\subseteq\; \operatorname{Spec}(R) \;\subseteq\; \operatorname{Srad}(R)$$

(2.25) Proposition: (viz. 886)
Let $(R,+,\cdot)$ be a commutative ring once more and $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be an arbitrary ideal of R. Then we obtain the following additional properties:

(i) If $\mathfrak{a}$ is proper, then the radical of $\mathfrak{a}$ is the intersection of all prime ideals containing $\mathfrak{a}$. And of course this is just the same, as taking the intersection of all prime ideals minimal over $\mathfrak{a}$:

$$\begin{aligned}\sqrt{\mathfrak{a}} &= \bigcap \{\, \mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{a} \subseteq \mathfrak{p} \,\} \\ &= \bigcap \{\, \mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{a} \subseteq \mathfrak{p} \,\}_*\end{aligned}$$

(ii) In particular the nil-radical of R is just the intersection of all (minimal) prime ideals of R, formally

$$\mathrm{NIL}(R) = \sqrt{0} = \bigcap \mathrm{Spec}(R) = \bigcap \mathrm{Smin}(R)$$

(iii) The map $\mathfrak{a} \mapsto \sqrt{\mathfrak{a}}$ is a projection on the set of ideals of R (i.e. it is idempotent). To be explicit: For any ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ we find the following equality

$$\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}}$$

(iv) Given an arbitrary ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ and a prime ideal $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ then for any $k \in \mathbb{N}$ we get the implication

$$\mathfrak{a}^k \subseteq \mathfrak{p} \subseteq \sqrt{\mathfrak{a}} \implies \mathfrak{p} = \sqrt{\mathfrak{a}}$$

(v) If $\mathfrak{a}$ and $\mathfrak{b} \trianglelefteq_{\mathrm{i}} R$ are any two ideals of R, then the radical of the product $\mathfrak{ab}$ equals the radical of the intersection $\mathfrak{a} \cap \mathfrak{a}$, which is the intersections of the radicals again:

$$\sqrt{\mathfrak{a}\,\mathfrak{b}} = \sqrt{\mathfrak{a} \cap \mathfrak{b}} = \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$$

(vi) And thereby, for any $1 \leq n \in \mathbb{N}$ we find that the radical of the power $\mathfrak{a}^n$ is just the radical of $\mathfrak{a}$:

$$\sqrt{\mathfrak{a}^n} = \sqrt{\mathfrak{a}}$$

In particular: If $\mathfrak{a} \in \mathrm{Srad}(R)$ is a radical ideal already and $1 \leq n \in \mathbb{N}$, again then the radical of any power $\mathfrak{a}^n$ is just $\mathfrak{a}$ again. Formally this reads, as

$$\sqrt{\mathfrak{a}^n} = \mathfrak{a}$$

(vii) Let $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be a finitely generated ideal in the commutative ring $(R,+,\cdot)$. And let $\mathfrak{b} \trianglelefteq_{\mathrm{i}} R$ be any another ideal of R. Then we get the implication

$$\mathfrak{a} \subseteq \sqrt{\mathfrak{b}} \implies \exists\, k \in \mathbb{N} \,:\, \mathfrak{a}^k \subseteq \mathfrak{b}$$

(viii) Consider an arbitrary family of ideals $\mathfrak{a}_i \trianglelefteq_{\mathrm{i}} R$ (where $i \in I$ and $I \neq \emptyset$ is any non-empty set of indices), then we obtain the following two inclusions

$$\begin{aligned} \sum_{i\in I} \sqrt{\mathfrak{a}} &\subseteq \sqrt{\sum_{i\in I} \mathfrak{a}_i} \\ \sqrt{\bigcap_{i\in I} \mathfrak{a}_i} &\subseteq \bigcap_{i\in I} \sqrt{\mathfrak{a}_i} \end{aligned}$$

(2.26) Remark:
Due to (2.22.(v)) the intersection of radical ideals yields a radical ideal. And in (2.24) we have just seen that maximal and prime ideals already are radical. Now recall that the *jacobson-radical* $\textsc{jac}(R)$ has been defined to be the intersection of all maximal ideals. And we have just seen in (2.25.(ii)) above that the *nil-radical* is the intersection of all (minimal) prime ideals. This means that both are radical ideals (and hence the word *radical* in their names)

$$\begin{aligned} \textsc{jac}(R) &= \bigcap \mathrm{Smax}(R) \in \mathrm{Srad}(R) \\ \textsc{nil}(R) &= \bigcap \mathrm{Spec}(R) \in \mathrm{Srad}(R) \end{aligned}$$

(2.27) Example:
Note however, that taking sums and radicals of (even finitely many) ideals do *not* commute. That is there is *no* analogous statement to (2.25.(v)) concerning sums $\mathfrak{a} + \mathfrak{b}$. As an example consider $R := E[s,t]$, the polynomial ring in two variables, where $(E, +, \cdot)$ is an arbitrary field. Now pick up

$$\mathfrak{p} := (s^2 - t)R \quad \text{and} \quad \mathfrak{q} := tR$$

It is clear that $\mathfrak{p}$ and $\mathfrak{q}$ are prime ideals (as the quotient is isomorphic to the integral domain $E[s]$ under the isomorphisms induced by $f(s,t) \mapsto f(s,s^2)$ and $f(s,t) \mapsto f(s,0)$ respectively). However the sum $\mathfrak{p} + \mathfrak{q}$ of both not even is a radical ideal, in fact we get

$$\mathfrak{p} + \mathfrak{q} = s^2R + tR \subset sR + tR = \sqrt{\mathfrak{p} + \mathfrak{q}}$$

Prob We first prove $\mathfrak{p} + \mathfrak{q} = s^2R + tR$ - thus consider any $h = (s^2 - t)f + tg \in \mathfrak{p} + \mathfrak{q}$, then h can be rewritten as $h = s^2f + t(g - f) \in s^2R + tR$. But conversely $t \in \mathfrak{q} \subseteq \mathfrak{p} + \mathfrak{q}$ and $s^2 = (s^2 - t) + t \in \mathfrak{p} + \mathfrak{q}$. In particular s is contained in the radical of $\mathfrak{p} + \mathfrak{q}$ and hence $\mathfrak{p} + \mathfrak{q} \subseteq sR + tR \subseteq \sqrt{\mathfrak{p} + \mathfrak{q}}$. As $sR + tR$ is prime (even maximal) this implies the equality of the radical ideal. So finally we wish to prove $s \notin \mathfrak{p} + \mathfrak{q}$ (and in particlar $\mathfrak{p} + \mathfrak{q}$ is no radical ideal. Thus suppose $s = s^2f + tg$ for some polynomials $f, g \in R$. Then (as s is prime and does not divide t) s divides g. To be precise we get $g = sh$ for $h = (1 - st)/t \in R$. And hence we get $s = s^2f + sth$. Eliminating s we find $1 = sf + th$, an equation that cannot hold true (as 1 is of degree 0 and $sf + th$ of degree at least 1). Thus we got $s^2 \notin s^2R + tR$.

(2.28) Example: (viz. 888)
Be aware that radicals may be very large when compared with their original ideals. E.g. it may happen that $\mathfrak{a} = aR$ is a principal ideal, but $\sqrt{\mathfrak{a}}$ is *not* finitely generated. In fact in the chapter of proofs we give an example where there even is no $n \in \mathbb{N}$ such that $(\sqrt{\mathfrak{a}})^n \subseteq \mathfrak{a}$, as well.

(2.29) Remark:
Combining (2.22.(iii)) and (viii) in the above proposition it is clear that for an arbitrary collection of ideals $\mathfrak{a}_i \trianglelefteq_{\mathrm{i}} R$ (where $i \in I$) in a commutative ring $(R, +, \cdot)$ we obtain the following equalities

$$\begin{aligned} \sqrt{\sum_{i\in I} \sqrt{\mathfrak{a}}} &= \sqrt{\sum_{i\in I} \mathfrak{a}_i} \\ \sqrt{\bigcap_{i\in I} \sqrt{\mathfrak{a}_i}} &= \sqrt{\bigcap_{i\in I} \mathfrak{a}_i} \end{aligned}$$

(2.30) Example:
The inclusions in (2.25.(viii)) need *not* be equalities! As an example let us consider the ring of integers $R = \mathbb{Z}$. And let us take $I = \mathbb{N}$ and $\mathfrak{a}_i = p^i\mathbb{Z}$ for some prime number $p \in \mathbb{Z}$. As any non-zero element of $\mathbb{Z}$ is divisible by finite powers p^i only the intersection of the $\mathfrak{a}_i$ is $\{0\}$. On the other hand $\sqrt{\mathfrak{a}_i} = p\mathbb{Z}$ due to (2.25.(vii)) and since $p\mathbb{Z}$ is a prime (and hence radical) ideal of $\mathbb{Z}$. Thereby we found the counterexample

$$\sqrt{\bigcap_{i\in\mathbb{N}} \mathfrak{a}_i} = \sqrt{0} = 0 \subset p\mathbb{Z} = \bigcap_{i\in\mathbb{N}} p\mathbb{Z} = \bigcap_{i\in\mathbb{N}} \sqrt{\mathfrak{a}_i}$$

(2.31) Proposition: (viz. 889)
Let now $\varphi : R \to S$ be a ring-homomorphism between the commutative rings $(R, +, \cdot)$ and $(S, +, \cdot)$. And consider the ideals $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ and $\mathfrak{b} \trianglelefteq_{\mathrm{i}} S$. Then let us denote the transferred ideals of $\mathfrak{a}$ and $\mathfrak{b}$

$$\begin{aligned} \mathfrak{b} \cap R &:= \varphi^{-1}(\mathfrak{b}) \trianglelefteq_{\mathrm{i}} R \\ \mathfrak{a}S &:= \langle \varphi(\mathfrak{a}) \rangle_{\mathrm{i}} \trianglelefteq_{\mathrm{i}} S \end{aligned}$$

Note that in case that φ is surjective (but in generall), we get $\mathfrak{a}S = \varphi(\mathfrak{a})$. Now, using these notions, we obtain the following four statements

(i) Pulling back ideals commutes with taking radical ideals, that is the radical of the pull-back of $\mathfrak{b}$ is just the pull-back of the radical of $\mathfrak{b}$

$$\sqrt{\mathfrak{b} \cap R} = \sqrt{\mathfrak{b}} \cap R$$

(ii) This is not true for the push-out of ideals, here we only find: The push-out of the radical ideal of $\mathfrak{a}$ is contained in the radical of the push-out of $\mathfrak{a}$

$$\sqrt{\mathfrak{a}}S \subseteq \sqrt{\mathfrak{a}S} = \sqrt{\sqrt{\mathfrak{a}}S}$$

(iii) Now let us abbreviate by $\star$ any of the properties *maximal ideal*, *prime ideal* or *radical ideal*. Then we find the equivalences

$$\mathfrak{b} \text{ is a } \star \iff \mathfrak{b} \cap R \text{ is a } \star$$

And if $\varphi : R \twoheadrightarrow S$ even is a surjective homomorphism, then we obtain another set of equivalences of

$$\mathfrak{a} + \ker(\varphi) \text{ is a } \star \iff \mathfrak{a}S \text{ is a } \star$$

(2.32) Remark:
Let $(R, +, \cdot)$ be a commutative ring and let us introduce the following maps on the set of ideals of R, respectively on the set of subsets of the spectrum of R

$$\mathbb{V} : \operatorname{Ideal}(R) \to \mathcal{P}\big(\operatorname{Spec}(R)\big) : \mathfrak{a} \mapsto \{\, \mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{a} \subseteq \mathfrak{p} \,\}$$
$$\mathbb{I} : \mathcal{P}\big(\operatorname{Spec}(R)\big) \to \operatorname{Ideal}(R) : \mathcal{X} \mapsto \begin{cases} \bigcap \mathcal{X} \text{ if } \mathcal{X} \neq \emptyset \\ R \text{ if } \mathcal{X} = \emptyset \end{cases}$$

Clearly these sets are partially ordered under inclusion, that is $(\operatorname{Ideal}(R), \subseteq)$ and $(\mathcal{P}(\operatorname{Spec}(R)), \subseteq)$ are partially ordered sets. Also it is clear that $\mathbb{V}$ and $\mathbb{I}$ are anti-tonous (aka order-reversing), that is for any $\mathfrak{a}, \mathfrak{b} \trianglelefteq_{\mathrm{i}} R$ and any $\mathcal{X}, \mathcal{Y} \subseteq \operatorname{Spec}(R)$ we find that

$$\mathfrak{a} \subseteq \mathfrak{b} \implies \mathbb{V}(\mathfrak{b}) \subseteq \mathbb{V}(\mathfrak{a})$$
$$\mathcal{X} \subseteq \mathcal{Y} \implies \mathbb{I}(\mathcal{Y}) \subseteq \mathbb{I}(\mathcal{X})$$

Recall the notion of a Galois connection introduced in (0.22). In (2.25.(i)) we have seen that $(\mathbb{V}, \mathbb{I})$ is a Galois connection between $(\operatorname{Ideal}(R), \subseteq)$ and $(\mathcal{P}(\operatorname{Spec}(R)), \subseteq)$, as these maps satisfy

$$\mathfrak{a} \subseteq \sqrt{\mathfrak{a}} = \mathbb{I}\mathbb{V}(\mathfrak{a})$$
$$\mathcal{X} \subseteq \mathbb{V}\mathbb{I}(\mathcal{X})$$

[the latter property being trivial, as $\bigcap \mathcal{X} \subseteq \mathfrak{p}$ for any $\mathfrak{p} \in \mathcal{X}$]. As with any Galois connection $\mathbb{V}$ and $\mathbb{I}$ now provide a one-to-one correspondence between their respective images, in this case these are

$$\operatorname{Srad}(R) = \operatorname{im}(\mathbb{I})$$
$$\mathcal{Z}_R := \operatorname{im}(\mathbb{V})$$

Thereby $\mathcal{Z}_R$ contains $\mathbb{V}(0) = \operatorname{Spec}(R)$ and $\mathbb{V}(R) = \emptyset$ and is closed under finite unions and arbitrary intersections, as we have seen in (2.16). In section 8.8 we will use these properties to introduce the so-called the *Zariski topology* on $\operatorname{Spec}(R)$ by taking $\mathcal{T}_R := \{\, \complement\mathbb{V}(\mathfrak{a}) \mid \mathfrak{a} \trianglelefteq_{\mathrm{i}} R \,\}$ to be the collection of open sets on $\operatorname{Spec}(R)$. This is possible, since we have

$$\mathbb{V}\left(\sum_{i \in I} \mathfrak{a}_i\right) = \bigcap_{i \in I} \mathbb{V}(\mathfrak{a}_i)$$
$$\mathbb{V}\left(\bigcap_{i=1}^{n} \mathfrak{a}_i\right) = \bigcup_{i=1}^{n} \mathbb{V}(\mathfrak{a}_i)$$

Jacobson Rings

The Jacobson property is an elementary notion and while it looks innocuous, it in fact is a rather strong assumption, that few rings satisfy. The integers $\mathbb{Z}$ and any field is a Jacobson ring. However this notion has excellent hereditary properties – it transfers to polynomial rings and epimorphic images and hence to finitely generated algebras (2.172). We will find that Hilbert rings are an equivalent notion in section 2.13, that are of special interest in polynomial rings. But we are getting ahead of ourselves – let us start with a definition that already contains several conditions, that all are equivalent:

(2.33) Definition: (viz. 890)

Let $(R,+,\cdot)$ be a commutative ring, then the following six properties for R are equivalent. And if R satisfies one (and hence all) of them, R is said to be a **Jacobson ring** or simply to be **jacobson**.

(a) The radical of any proper ideal is the intersection of maximal ideals of R. That is: For any ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ with $\mathfrak{a} \neq R$ there is a non-empty set $\mathcal{M} \subseteq \operatorname{Smax}(R)$, such that

$$\sqrt{\mathfrak{a}} \;=\; \bigcap \mathcal{M}$$

(b) The radical of any proper ideal is the intersection of the maximal ideals of R containing it. That is: For any ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ with $\mathfrak{a} \neq R$ we get the identity

$$\sqrt{\mathfrak{a}} \;=\; \bigcap \{\, \mathfrak{m} \in \operatorname{Smax}(R) \mid \mathfrak{a} \subseteq \mathfrak{m} \,\}$$

(c) Any prime ideal is the intersection of the maximal ideals of R containing it. That is: For any prime ideal $\mathfrak{p} \in \operatorname{Spec}(R)$ we get the identity

$$\mathfrak{p} \;=\; \bigcap \{\, \mathfrak{m} \in \operatorname{Smax}(R) \mid \mathfrak{p} \subseteq \mathfrak{m} \,\}$$

(d) For any ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ the Jacobson-radical and nil-radical of the quotient ring $R/\mathfrak{a}$ coincide, i.e.

$$\operatorname{JAC}\left(R \big/ \mathfrak{a}\right) \;=\; \operatorname{NIL}\left(R \big/ \mathfrak{a}\right)$$

(e) For any prime ideal $\mathfrak{p} \in \operatorname{Spec}(R)$ the Jacobson-radical of the quotient ring $R/\mathfrak{p}$ vanishes, that is

$$\operatorname{JAC}\left(R \big/ \mathfrak{p}\right) \;=\; 0$$

(f) If $(S,+,\cdot)$ is an integral domain and $\varphi : R \twoheadrightarrow S$ is a surjective homomorphism of rings, then the Jacobson-radical of S vanishes, formally

$$\operatorname{JAC}(S) \;=\; 0$$

Nota By (2.25.(i)) the radical $\sqrt{\mathfrak{a}}$ of an ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ is the intersection of all *prime* ideals containing $\mathfrak{a}$. Now property (b) tells us, that the defining property of a Jacobson ring is, that this is the same as the intersection of all *maximal* ideals containing $\mathfrak{a}$. This is a strong restriction.

2.4 Noetherian Rings

In this section we will introduce and study noetherian and artinian rings. Both types of rings are defined by a chain condition on ideals - ascending in the case of noetherian and descending in the case of artinian rings. So one might expect a completely dual theory for these two objects. Yet this is not the case! In fact it turns out that the artinian property is much stronger: Any artinian ring already is noetherian, but the converse is false. And while examples of noetherian rings are abundant, there are few artinian rings. On the other hand both kinds of rings have several similar properties, e.g. both are very well-behaved under taking quotients or localizations.
Throughout the course of this book we will see that noetherian rings have lots of beautiful properties. E.g. they allow the Lasker-Noether decomopsition of ideals. However in non-noetherian rings peculiar things may happen. Together with the easy properties of inheritance this makes noetherian rings one of the predominant objects of commutative algebra and algebraic geometry. Artinian rings are of lesser importance, yet they arise naturally in number theory and the theory of algebraic curves.

(2.34) Definition: (viz. 1031)
Let $(R,+,\cdot)$ be a commutative ring, then R is said to be **noetherian** iff it satisfies one of the following five equivalent conditions

(a) R satisfies the *ascending chain condition* (ACC) of ideals - that is any family of ideals $\mathfrak{a}_k \trianglelefteq_{\mathfrak{i}} R$ of R (where $k \in \mathbb{N}$) that forms an ascending chain of ideals

$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \ldots \subseteq \mathfrak{a}_k \subseteq \mathfrak{a}_{k+1} \subseteq \ldots$$

becomes eventually constant - that is there is some $s \in \mathbb{N}$, such that the chain actually looks like

$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \ldots \subseteq \mathfrak{a}_s = \mathfrak{a}_{s+1} = \ldots$$

(b) Every non-empty family of ideals contains a maximal element, that is: Given $\mathcal{A} \subseteq \mathrm{Ideal}(R)$ such that $\mathcal{A} \neq \emptyset$ there is some $\mathfrak{a}^* \in \mathcal{A}^*$ (i.e $\forall\, \mathfrak{a} \in \mathcal{A}$ we get $\mathfrak{a}^* \subseteq \mathfrak{a} \implies \mathfrak{a}^* = \mathfrak{a}$).

(c) If $(\mathfrak{a}_i) \subseteq \mathrm{Ideal}(R)$ is an arbitrary collection (i.e. $i \in I$ for an arbitrary set $I \neq \emptyset$) of ideals of R, then there is a finite subset $\Omega \subseteq I$ such that

$$\sum_{i \in I} \mathfrak{a}_i = \sum_{i \in \Omega} \mathfrak{a}_i$$

(d) Every ideal of R is finitely generated, formally that is: For any ideal $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$ there are some $a_1, \ldots, a_k \in R$ such that we get

$$\mathfrak{a} = \langle a_1, \ldots, a_k \rangle_{\mathfrak{i}} = a_1 R + \cdots + a_k R$$

(e) Every prime ideal of R is finitely generated, formally that is: For any prime ideal $\mathfrak{p} \in \mathrm{Spec}(R)$ there are some $a_1, \ldots, a_k \in R$ such that

$$\mathfrak{p} = \langle a_1, \ldots, a_k \rangle_{\mathfrak{i}} = a_1 R + \cdots + a_k R$$

Note that the equivalence of (a) and (b) is true for any partially ordered set $(X, \leq)$, due to (0.25). So this is just the special case of the set of ideals partially ordered under inclusion $(\mathrm{Ideal}(R), \subseteq)$. Properties (c) and (d) are a specialty of ideals in rings however. ACC gives rise to method of proving statements that is similar to induction:

(2.35) Remark: Noetherian Induction:
Let $(R, +, \cdot)$ be noetherian ring and P be a predicate on the set of ideals of R - i.e. $P(\mathfrak{a})$ either is *true* or *false*. Consider an arbitrary collection $\mathcal{A} \subseteq \mathrm{Ideal}(R)$ of ideals of R. In order to prove that P holds true for all $\mathfrak{a} \in \mathcal{A}$, it suffices to prove the following

$$\forall\, \mathfrak{a} \in \mathcal{A} \,:\, \neg P(\mathfrak{a}) \implies \exists\, \mathfrak{b} \in \mathcal{A} \,:\, \mathfrak{a} \subset \mathfrak{b} \text{ and } \neg P(\mathfrak{b})$$

Prob if there was some $\mathfrak{a}_0 \in \mathcal{A}$ such that $P(\mathfrak{a}_0)$ was false, then there was some $\mathfrak{a}_1 := \mathfrak{b} \in \mathcal{A}$ such that $\mathfrak{a}_0 \subset \mathfrak{a}_1$ and $P(\mathfrak{a}_1)$ is false again. Then we find $\mathfrak{a}_2 := \mathfrak{b}$ with $\mathfrak{a}_1 \subset \mathfrak{a}_2$ and $\neg P(\mathfrak{a}_2)$. Continuing this way, we would end up with a strictly increasing chain $\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots$ of ideals, contradicting ACC.

(2.36) Example: $(\diamondsuit)$
A word of warning for the reader, who has some previous knowledge of algebraic geometry: If R is a noetherian ring, then $X := \mathrm{Spec}(R)$ is a noetherian topological space. The converse need *not* be true however. If X is a noetherian topological space, then R has to satisfy ACC for all radical ideals only. This however does not imply ACC for *all* ideals however, which is (a).

Let us present a counterexample: A ring R that satifies ACC for radical ideals (i.e. for ideals $\mathfrak{u} \trianglelefteq_{\mathfrak{i}} R$ with $\sqrt{\mathfrak{u}} = \mathfrak{u}$) but not for all ideals. We head out with any field F and take $A := F[t_0, t_1, \ldots]$ the polynomial ring in countably many variables. Now pick up the ideal of A generated by

$$\mathfrak{a} \;:=\; \langle t_k^2 - t_{k-1} \mid 1 \leq k \in \mathbb{N} \rangle_{\mathfrak{i}}$$

The evil ring is the quotient $R := A/\mathfrak{a}$. Let us abbreviate $x_k := t_k + \mathfrak{a}$, then by construction we have $x_k^2 = t_k^2 + \mathfrak{a} = t_{k-1} + \mathfrak{a} = x_{k-1}$. That is x_k is the square root of x_{k-1}. In particular $x_{k-1}R \subset x_kR$ and thereby R is not noetherian, as

$$x_0R \;\subset\; x_1R \;\subset\; x_2R \;\subset\; \ldots$$

However any $f + \mathfrak{a} \in R$ only has finitely many variables $f(t_0, \ldots, t_n)$ so $f + \mathfrak{a} = f(x_0, x_1, \ldots, x_n) \in R$. Also it has finitely many summands only. From this we see (using the polynomial rule) that $(f + \mathfrak{a})^{2n} \in F[x_0] \subseteq R$, that is for any $v = f + \mathfrak{a} \in R$ there is some $m \in \mathbb{N}$ such that $v^m \in F[x_0]$. Now consider any ascending chain of radical ideals $\sqrt{\mathfrak{u}_k} = \mathfrak{u}_k$:

$$\mathfrak{u}_0 \;\subseteq\; \mathfrak{u}_1 \;\subseteq\; \mathfrak{u}_2 \;\subseteq\; \ldots$$

This chain induces an ascending chain of ideals in $F[x_0]$, by taking $\mathfrak{a}_k := \mathfrak{u}_k \cap F[x_0] \trianglelefteq_{\mathfrak{i}} F[x_0]$. Note that $\mathfrak{a}_{k-1} = \mathfrak{a}_k$ implies $\mathfrak{u}_{k-1} = \mathfrak{u}_k$, as: Choose any $v \in \mathfrak{u}_k$ then there is some $m \in \mathbb{N}$ such that $v^m \in F[x_0]$ and hence $v^m \in \mathfrak{u}_k \cap F[x_0] = \mathfrak{a}_k = \mathfrak{a}_{k-1} = \mathfrak{u}_{k-1} \cap F[x_0]$. But $v^m \in \mathfrak{u}_{k-1}$ means $v \in \sqrt{\mathfrak{u}_{k-1}} = \mathfrak{u}_{k-1}$ such that we have $\mathfrak{u}_k \subseteq \mathfrak{u}_{k-1}$, too.

Yet $F[x_0]$ is a noetherian ring, such that the chain $\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \ldots$ stabilizes. But as we have just argued, this implies, that the original chain $\mathfrak{u}_0 \subseteq \mathfrak{u}_1 \subseteq \mathfrak{u}_2 \subseteq \ldots$ has to stabilize, as well. Thus R satisfies ACC for all chains of radical ideals, even though it is not a noetherian ring.

The dual property DCC of ACC on ideals gives rise to another interesting notion: Commutative rings satisfying DCC on ideals will be called *artinian*. And again we find an even longer list of equivalent statements. The similarity in the definition gives strong reason to study these objects simultaneously. But as often only one half of the equivalences can be proved straightforwardly while the other half requires heavy-duty machinery that is not yet available. For a novice reader it might hence be wise to concentrate on noetherian rings only, for now. These will be the important objects later on.

(2.37) Definition: (viz. 908)
Let $(R, +, \cdot)$ be a commutative ring, then R is said to be **artinian** iff it satisfies one of the following six equivalent conditions

(a) R satisfies the *descending chain condition* (DCC) of ideals - that is any family of ideals $\mathfrak{a}_k \trianglelefteq_{\mathfrak{i}} R$ of R (where $k \in \mathbb{N}$) that forms a descending chain of ideals

$$\mathfrak{a}_0 \supseteq \mathfrak{a}_1 \supseteq \ldots \supseteq \mathfrak{a}_k \supseteq \mathfrak{a}_{k+1} \supseteq \ldots$$

becomes eventually constant - that is there is some $s \in \mathbb{N}$ such that the chain actually looks like

$$\mathfrak{a}_0 \supseteq \mathfrak{a}_1 \supseteq \ldots \supseteq \mathfrak{a}_s = \mathfrak{a}_{s+1} = \ldots$$

(b) Every non-empty family of ideals contains a minimal element, that is: Given $\mathcal{A} \subseteq \mathrm{Ideal}(R)$ such that $\mathcal{A} \neq \emptyset$ there is some $\mathfrak{a}_* \in \mathcal{A}_*$ (i.e $\forall\, \mathfrak{a} \in \mathcal{A}$ we get $\mathfrak{a} \subseteq \mathfrak{a}_* \implies \mathfrak{a} = \mathfrak{a}_*$).

(c) If $\mathcal{A} \subseteq \mathrm{Ideal}(R)$ is a family of ideals, that is totally ordered under inclusion $\subseteq$ of sets (i.e for any $\mathfrak{a}, \mathfrak{b} \in \mathcal{A}$ we have $\mathfrak{a} \subseteq \mathfrak{b}$ or $\mathfrak{b} \subseteq \mathfrak{a}$), then $\mathcal{A}$ has to be finite.

(d) R is of finite length as an R-module - that is there is an upper bound on the maximal length of a strictly ascending chain of ideals, formally

$$\ell(R) := \sup \left\{ k \in \mathbb{N} \;\middle|\; \begin{array}{l} \exists\, \mathfrak{a}_0, \mathfrak{a}_1, \ldots, \mathfrak{a}_k \trianglelefteq_{\mathfrak{i}} R : \\ \mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \ldots \subset \mathfrak{a}_k \end{array} \right\} < \infty$$

(e) R is a noetherian ring in which any prime ideal already is maximal, in terms of the spectra of R:

$$\mathrm{Smax}(R) = \mathrm{Spec}(R)$$

(f) R is a noetherian ring, whose Jacobson radical equals its nil-radical [i.e. $\textsc{jac}(R) = \textsc{nil}(R)$] and that is semi-local [i.e. $\#\mathrm{Smax}(R) < \infty$].

(2.38) Remark:
So what does the noetherian resp. the artinian property mean? This can best be seen by considering a chain of principal ideals $\mathfrak{a}_k = a_k R$ of some commutative ring R. For these an ascending chain

$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \ldots \subseteq \mathfrak{a}_k \subseteq \mathfrak{a}_{k+1} \subseteq \ldots \subseteq R$$

is nothing but the chain of divisibilities of the elements $a_1 \mid a_0$, $a_2 \mid a_1$ and so on, such that altogether we have $\ldots\ a_{k+1} \mid a_k \mid \ldots \mid a_2 \mid a_1 \mid a_0$. It is well known, that e.g. for the integers $R = \mathbb{Z}$ any number $a = a_0 \in R$ only has finitely many divisors. Hence the chain of divisibilities has to stabilize $\ldots = a_{s+1} = a_s \mid \ldots \mid a_2 \mid a_1 \mid a_0$ at some index $s \in \mathbb{N}$. And this is precisely what the noetherian property needs:

$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \ldots \subseteq \mathfrak{a}_s = \mathfrak{a}_{s+1} = \ldots$$

In other words the integers $\mathbb{Z}$ are an example of a noetherian ring, since the only ideals of $\mathbb{Z}$ are principal ideals. It is worth to note, that there are rings that actually contain elements with ininitely many divisors, e.g. the ring $\mathbb{R}\{x\}$ of analytic functions over $\mathbb{R}$ allows the decomposition

$$\sin(x) = x \cdot \prod_{k=1}^{\infty} \left(1 - \frac{x^2}{k^2\pi^2}\right)$$

found by Leonhard Euler. In particular $\mathbb{R}\{x\}$ cannot be a noetherian ring. Likewise a descending chain of principal ideals $\mathfrak{a}_k = a_k R$

$$\mathfrak{a}_0 \supseteq \mathfrak{a}_1 \supseteq \ldots \supseteq \mathfrak{a}_k \subseteq \mathfrak{a}_{k+1} \supseteq \ldots \subseteq R$$

turns into an ascending chain of divivibilities $a_0 \mid a_1 \mid a_2 \mid \ldots \mid a_k \mid a_{k+1} \mid \ldots$. This is something which is easily possible in the integers, polynomials and most other rings - just keep multiplying non-unit elements. The numbers a_k will get larger, but there is no upper bound.

In case of an artinian ring however, this chain has to stabilize which means that there is some $s \in \mathbb{N}$ such that $a_s R = a_{s+1} R = \ldots$. In particular for $a_k := a^k$ for some fixed $a \in R$ we have $a^s \in a^s R = a^{s+1} R$. Thus there has to be some $u \in R$ such that $a^s = a^{s+1} u$ or in other words $a^{s+1}(au - 1) = 0$. If a is a non-zero-divisor, so is a^s such that in this case we would have $au = 1$. For this reason in an artinian ring R any non-zero-divisor already is a unit

$$R \text{ artinian} \quad \Longrightarrow \quad \text{NZD}(R) = R^*$$

From this it is clear that being an artinian ring already is a really strong property. And it is also clear, that it is hard to find examples of artinian rings that are not fields or finite rings. The artinian property lies in the zero-divisors of the ring. In consequence artinian rings not only are far less common but they also are severely more difficult to handle than noetherian rings.

(2.39) Example:

- Any field E is an noetherian and artinian ring, as it only contains the trivial ideals 0 and E. In particular the only chain of ideals with strict inclusions is $0 \subset E$ and this is finite.

- Any finite ring - such as $\mathbb{Z}_n$ - is artinian and noetherian, as it only contains finitely many ideals (and in particular any infinity chain of ideals has to be eventually constant).

- We will study principal ideal domains (PIDs) in section 2.7. These are integral domains R in which every ideal $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$ is generated by some element $a \in R$ (that is $\mathfrak{a} = aR$). In particular any ideal is finitely generated and hence any PID is noetherian.

- The integers $\mathbb{Z}$ form an easy example of a noetherian ring (as they are a PID). But they are not artinian, e.g. they contain the infinitely decreasing chain of ideals generated by powers of 2: $\mathbb{Z} \supset 2\mathbb{Z} \supset 4\mathbb{Z} \supset 8\mathbb{Z} \supset \ldots \supset 2^k\mathbb{Z} \supset \ldots$

- We will soon see (a special case of the Hilbert basis theorem) that the polynomial ring $R = E[t_1, \ldots, t_n]$ in finitely many variables over a field E is a noetherian ring. And again this is no artinian ring, as it contains the infinitely decreasing chain of ideals $R \supset t_1 R \supset t_1^2 R \supset \ldots$

- Of course there are examples of non-noetherian rings, too. E.g. let E be a field and consider $R := E[t_i \mid 1 \leq i \in \mathbb{N}]$ the polynomial ring in (countably) infinitely many indeterminates. Then R is an integral domain but it is not noetherian. Just let $\mathfrak{p}_k := \langle t_1, t_2, \ldots, t_k \rangle_{\mathfrak{i}}$ be the prime ideal generated by the first k indeterminates. Then we obtain an infinitely ascending chain of (even prime) ideals $\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \ldots \subset \mathfrak{p}_k \subset \ldots$

- Non-noetherian rings may well lie inside of noetherian rings: As an example regard the ring $R = E[t_i \mid 1 \leq i \in \mathbb{N}]$ again. As R is an integral domain R is contained in its quotient field F. But as F is a field it in particular is noetherian.

- The standard example of an artinian ring in algebraic geometry is the following: Let R be a noetherian ring, e.g. $R = E[t_1, \ldots, t_n]$, where E is a field. Now pick up finitely many maximal ideals $\mathfrak{m}_1$ to $\mathfrak{m}_r$ of R and let $\mathfrak{j} := \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r$. Geometrically speaking any maximal ideal corresponds to a point and the intersection to the union of these. Then $A := R/\mathfrak{j}$ is an artinian ring: It is noetherian since R is and its only has the maximal ideals $\mathfrak{m}_i/\mathfrak{j}$. By construction these are only finitely many and it satisfies $\textsc{jac}(A) = \mathfrak{j}/\mathfrak{j} = 0 \subseteq \textsc{nil}(A) \subseteq \textsc{jac}(A)$. Hence A satisfies all the properties required in (e).

- As a counterexample consider the maximal ideal $\mathfrak{m} = \langle t_i \mid i \in \mathbb{N} \rangle_{\mathfrak{i}}$ in the polynomial ring of infinitely many variables $R = E[t_i \mid i \in \mathbb{N}]$ over the field E. Then the ring $S := R/\mathfrak{m}^2$ is not noetherian but only has maximal prime ideals (it is of Krull-dimension 0).

- ($\diamondsuit$) Another example from complex analysis: Let $\mathcal{O} := \{ f : \mathbb{C} \to \mathbb{C} \mid f \text{ holomorphic} \}$ be the ring of holomorphic functions on $\mathbb{C}$ [that this is isomorphic to the ring $\mathbb{C}\{z\}$ of globally convergent power series]. Now let $\mathfrak{a}_k := \{ f \in \mathcal{O} \mid \forall k \leq n \in \mathbb{N} : f(n) = 0 \}$. Clearly the $\mathfrak{a}_k \trianglelefteq_{\mathfrak{i}} \mathcal{O}$ are ideals of $\mathcal{O}$ they even form a strictly ascending chain of ideals (this is a special case of the Weierstrass product theorem). Again $\mathcal{O}$ is an integral domain (by the identity theorem of holomorphic functions) but - as we have just seen, or by the Weierstrass factorisation theorem - it is not noetherian.

(2.40) Proposition: (viz. 1033)
Let $(R,+,\cdot)$ be a commutative ring and fix $\star$ as an abbreviation for either of the words *noetherian* or *artinian*. Then the following statements hold true:

(i) If $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ is an ideal and R is $\star$, then the quotient $R/\mathfrak{a}$ also is a $\star$ ring.

(ii) Let $(S,+,\cdot)$ be any ring and let $\varphi : R \twoheadrightarrow S$ be a surjective ring-homomorphism. If now R is a $\star$ ring, then S is a $\star$ ring, too.

(iii) Suppose R and S are commutative rings. Then the direct sum $R \oplus S$ is a $\star$ ring if and only if both R and S are $\star$ rings.

(2.41) Remark:
We are about to formulate Hilbert's basis theorem. Yet in order to do this we first straighten out a few things for the reader who is not familiar with the notion of an R-algebra. Consider a commutative ring $(S,+,\cdot)$ and a sub-ring $R \leq_{\mathrm{r}} S$ of it. Further let $E \subseteq S$ be any subset, then we introduce the R-sub-ring of S *generated* by E to be the following

$$R[E] := \left\{ \sum_{i=1}^{m} a_i \prod_{j=1}^{n} e_{i,j} \;\middle|\; m,n \in \mathbb{N},\ a_i \in R, e_{i,j} \in E \right\}$$

Nota that $0 \in R[X]$ as $m = 0$ and $1 \in R[E]$ as $n = 0$ are allowed. And thereby $R[E]$ is a sub-ring of S, containing R. In fact $R[E]$ is precisely the R-subalgebra of S generated by E in the sense of section 3.2. And for those who already know the notion of polynomials in several variables this can also be put in the following form

$$R[E] = \{ f(e_1,\ldots,e_n) \mid 1 \leq n \in \mathbb{N},\ f \in R[t_1,\ldots,t_n],\ e_i \in E \}$$

In particular if E is a finite set - say $E = \{ e_1,\ldots,e_n \}$ - we also write $R[e_1,\ldots,e_n] := R[E]$. And this is just the image of the polynomial ring $R[t_1,\ldots,t_n]$ under the evaluation homomorphism $t_i \mapsto e_i$.

(2.42) Theorem: (viz. 1035) **Hilbert Basis Theorem**
Let $(S,+,\cdot)$ be a commutative ring and consider a sub-ring $R \leq_{\mathrm{r}} S$. Further suppose that S is *finitely generated* (as an R-algebra) over R, that is there are finitely many $e_1,\ldots,e_n \in S$ such that $S = R[e_1,\ldots,e_n]$. If now R is a noetherian ring, then S is a noetherian ring, too

$$R \text{ noetherian} \quad\Longrightarrow\quad S = R[e_1,\ldots,e_n] \text{ noetherian}$$

($\diamondsuit$) An extension of this theorem is the *Noetherian Normalisation Theorem*, that we will formulate in section 8.4. It states that a finitely generated commutative algebra $A = F[e_1,\ldots,e_n]$ over a field F admits a sub-ring $S \leq_{\mathrm{r}} A$ such that $S \cong_{\mathrm{a}} F[t_1,\ldots,t_d]$ is isomorphic to a polynomial ring over F and A is finitely generated, as a module over S. However, for the time being, we have not introduced all the ingredients required for this.

(2.43) Remark:
The major work in proving Hilbert's Basis Theorem lies in regarding the polynomial ring $S = R[t]$. The rest is just induction and (2.40.(ii)). And for this we chose a constructive proof. That is given a non-zero ideal $0 \neq \mathfrak{u} \trianglelefteq_{\mathrm{i}} S$ we want to find a finite set of generators of $\mathfrak{u}$. To do this let

$$\mathfrak{a}_k \;:=\; \{\, \mathrm{lc}(f) \mid f \in \mathfrak{u},\ \deg(f) = k \,\} \cup \{0\}$$

As $\mathfrak{a}_k$ is an ideal of R it is finitely generated, say $\mathfrak{a}_k = \langle a_{k,1}, \ldots, a_{k,n(k)} \rangle_{\mathrm{i}}$ where $a_{k,i} = f_{k,i}$ for some $f_{k,i} \in \mathfrak{u}$ with $\deg(f_{k,i}) = k$ and $a_{k,i} = \mathrm{lc}(f_{k,i})$. Further the $\mathfrak{a}_k$ form an ascending chain and hence there is some $s \in \mathbb{N}$ such that $\mathfrak{a}_s = \mathfrak{a}_{s+1} = \mathfrak{a}_{s+2} = \ldots$. Then a trick argument shows

$$\mathfrak{u} \;=\; \langle f_{k,1} \mid k \in 0 \ldots s,\ i \in 1 \ldots n(k) \rangle_{\mathrm{i}}$$

(2.44) Definition:
Let $(R, +, \cdot)$ be any commutative ring and $\mathfrak{q}_\circ$, $\mathfrak{q} \trianglelefteq_{\mathrm{i}} R$ be a prime ideals of R. Then we say that $\mathfrak{q}_\circ$ **lies directly** under $\mathfrak{q}$ if $\mathfrak{q}_\circ$ is maximal among the prime ideals contained in $\mathfrak{q}$. And we abbreviate this by writing $\mathfrak{q}_\circ \subset_* \mathfrak{q}$. Formally that is

$$\begin{aligned} \mathfrak{q}_\circ \subset_* \mathfrak{q} \quad &:\Longleftrightarrow \quad \mathfrak{q}_\circ \in \{\, \mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \subset \mathfrak{q} \,\}^* \\ &\Longleftrightarrow \quad (1)\ \ \mathfrak{q}_\circ \in \mathrm{Spec}(R) \text{ with } \mathfrak{q}_\circ \subset \mathfrak{q} \\ &\qquad\quad\ (2)\ \ \forall\ \mathfrak{p} \in \mathrm{Spec}(R)\ :\ \mathfrak{q}_\circ \subseteq \mathfrak{p} \subseteq \mathfrak{q} \implies \mathfrak{q}_\circ = \mathfrak{p} \text{ or } \mathfrak{p} = \mathfrak{q} \end{aligned}$$

(2.45) Proposition: (viz. 1037)
Let $(R, +, \cdot)$ be a noetherian ring, then we find the truth of the following four statements

(i) Any non-empty set of ideals of R contains a maximal element. That is for any $\mathcal{A} \subseteq \mathrm{Ideal}(R)$ with $\mathcal{A} \neq \emptyset$ there is some $\mathfrak{a}^* \in \mathcal{A}$ that satisfies the following property

$$\forall\, \mathfrak{a} \in \mathcal{A} \text{ we get } \mathfrak{a}^* \subseteq \mathfrak{a} \quad\Longrightarrow\quad \mathfrak{a}^* = \mathfrak{a}$$

(ii) Any non-empty set of prime ideals of R contains maximal and minimal elements. That is for any non-empty $\mathcal{P} \neq \emptyset$ set of prime ideals $\mathcal{P} \subseteq \mathrm{Spec}(R)$ of R we get

$$\mathcal{P}_* \neq \emptyset \quad \text{and} \quad \mathcal{P}^* \neq \emptyset$$

(iii) In particular for any two prime ideals $\mathfrak{p}$, $\mathfrak{q} \trianglelefteq_{\mathrm{i}} R$ with $\mathfrak{p} \subset \mathfrak{q}$ there is a prime ideal $\mathfrak{q}_\circ$ lying directly under $\mathfrak{q}$. Formally that is the following statement

$$\exists\ \mathfrak{q}_\circ \in \mathrm{Spec}(R)\ :\ \mathfrak{p} \subseteq \mathfrak{q}_\circ \subset_* \mathfrak{q}$$

(iv) Let $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be any proper ideal, i.e. $\mathfrak{a} \neq R$, then there only are finitely many prime ideals lying minimally over $\mathfrak{a}$. Formally that is the following statement

$$1 \;\leq\; \#\{\, \mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{a} \subseteq \mathfrak{p} \,\}_* \;<\; \infty$$

(2.46) Proposition: (viz. 906)
Let $(R, +, \cdot)$ be an artinian ring, then we find the truth of the following seven statements

(i) An artinian integral domain already is a field.

(ii) Any artinian ring already is a noetherian ring.

(iii) In an artinian ring R maximal, prime and minimal prime ideals all coincide, in terms of the spectra:

$$\mathrm{Smax}(R) \;=\; \mathrm{Spec}(R) \;=\; \mathrm{Smin}(R)$$

(iv) Any artinian ring already is semilocal, that is it only has finitely many maximal ideals.

(v) In an artinian ring the Jacobson radical and the nil-radical coincide and are nilpotent, put formally

$$\textsc{jac}(R) \;=\; \textsc{nil}(R) \quad \text{and} \quad \exists\, n \in \mathbb{N} : (\textsc{jac}(R))^n = 0$$

(vi) For an artinian ring R the reduction $R/\textsc{nil}(R)$ is isomorphic to the (finite) direct sum of its residue fields. And we can even give the isomorphism explicitly to be

$$R\Big/_{\textsc{nil}(R)} \;\cong_{\mathrm{r}}\; \bigoplus_{\mathfrak{m} \,\in\, \mathrm{smax}(R)} R\Big/_{\mathfrak{m}} \;:\; a + \textsc{nil}(R) \mapsto (a + \mathfrak{m})$$

(vii) An artinian ring R can be decomposed into a finite number of local artinian rings. That is there are local, artinian rings L_i such that we get an isomorphy

$$R \;\cong_{\mathrm{r}}\; L_1 \oplus \cdots \oplus L_r$$

Nota Thereby $r := \#\mathrm{Smax}(R)$ is the number of maximal ideals of R and any L_i is of the form $L_i = R/\mathfrak{m}_i^n$ where $n \in \mathbb{N}$ such that $(\textsc{jac}(R))^n = 0$. The isomorphism is natural: $a \mapsto (a + \mathfrak{m}_i^n)$.

(2.47) Corollary: (viz. 1036)
Let $(R, +, \cdot)$ be any commutative ring, then R is the union of a net of noetherian sub-rings. That is there is a family (R_i) (where $i \in I$) of sub-rings such that the following statements hold true

(1) $R_i \;\leq_{\mathrm{r}}\; R$ is a sub-ring for any $i \in I$

(2) R_i is a noetherian ring for any $i \in I$

(3) $R = \bigcup_{i \in I} R_i$

(4) $\forall\, i, j \in I \;\exists\, k \in I$ such that $R_i \cup R_j \;\subseteq\; R_k$

2.5 Unique Factorisation Domains

The reader most probably is aware of the fact, that any integer $n \in \mathbb{Z}$ (apart from 0) admits a decomposition into primes. In this and the next section we will study what kinds of rings qualify to have this property. We will see that noetherian integral domains come close, but do not suffice. And we will see that PIDs will allow prime decomposition. That is the truth lies somewhere in between but cannot be pinned down precisely.
According to the good, old traditions of mathematics we're in for a definition: A ring will simply said to be *factorial*, iff it allows prime decomposition (a mathematical heretic might object: "If you can't prove it, define it!"). Then PIDs are factorial. And the lemma of Gauss is one of the few answers in which cases the factorial property is preserved.
So we have to start with a lengthy series of (luckily very easy) definitions. But once we have assembled the language needed for prime decomposition we will be rewarded with several theorems of great beauty - the fundamental theorem of arithmetic at their center.

(2.48) Definition: (viz. 1038)
Let $(R, +, \cdot)$ be a commutative ring and $a, b \in R$ be two elements of R. Then we say that a **divides** b (written as $a \mid b$) iff one of the following three equivalent properties is satisfied

(a) $b \in aR$

(b) $bR \subseteq aR$

(c) $\exists\, h \in R \;:\; b = ah$

And we define the **order** of a in b to be the highest number $k \in \mathbb{N}$ such that a^k still divides b (if a^k divides b for any $k \in \mathbb{N}$, then the order of a in b is taken to be ∞)

$$\langle a \mid b \rangle \;:=\; \sup\Big\{\, k \in \mathbb{N} \mid b \in a^k R \,\Big\} \;\in\; \mathbb{N} \cup \{\infty\}$$

We say that a and b are **associated**, which we will denote as $a \approx b$ iff there is some unit $\alpha \in R^*$ such that $b = \alpha a$. And if R is an integral domain then $a \approx b$ is true, iff one of the following three equivalent properties is satisfied

(a) $aR = bR$

(b) $a \mid b$ and $b \mid a$

(c) $\exists\, \alpha \in R^* \;:\; b = \alpha a$

(2.49) Remark:

(i) By construction $\approx$ is an equivalence relation on R, that $\approx$ is a reflexive, symmetric and transitive relation. And for any $a \in R$ the equivalence class of $a \in R$ is given to be $[a] = R^* a := \{\, \alpha a \mid \alpha \in R^* \,\}$. In particular we have $[0] = 0$ and $[1] = R^*$.

Prob we have $a \approx a$, as $a = 1 \cdot a$ and if $b = \alpha a$ for some $\alpha \in R^*$ then also $a = \alpha^{-1} b$ such that $a \approx b$ also implies $b \approx a$. Finally if $a \approx b$ and $b \approx x$ then we have $b = \alpha a$ and $c = \beta b$ such that $c = \beta\alpha a$ and as $\beta\alpha \in R^*$ (with inverse $\alpha^{-1}\beta^{-1}$) again, this is $a \approx c$.

(ii) If R is an integral domain and $a, b \in R$ such that $a \neq 0$ and $a \mid b$ then the *divisor* $h \in R$ satisfying $b = ah$ is uniquely determined. As we sometimes wish to refer to the divisor, it deserves a name of its own. Hence if R is an integral domain, $a, b \in R$ with $a \neq 0$ and $a \mid b$ we let

$$\frac{a}{b} := h \quad \text{such that} \quad b = ah$$

Prob we have to show the uniqueness: Thus suppose $b = ag$ and $b = ah$ then $a(g - h) = 0$. And as $a \neq 0$ and R is an integral domain this yields $g - h = 0$ and hence $g = h$.

(2.50) Example:
Let $(R, +, \cdot)$ be an commutative ring and $a, b \in R$. Let us denote the ideal generated by a and b by $\mathfrak{a} := aR + bR$. Now consider any polynomial $f \in R[t]$, $1 \leq k \in \mathbb{N}$ and let $d := \deg(f)$. Then a straightforward computation yields

$$f(a)a^k - f(b)b^k \;=\; (a-b)\left(\sum_{i=0}^{d} f[i] \sum_{j=0}^{k-1+i} a^j b^{k-j}\right)$$

A special case of this is the third binomial rule $a^2 - b^2 = (a - b)(a + b)$ which is obtained by letting $f(t) := t$. Thus this cumbersome double sum on the right is the divisor of $f(a)a^k - f(b)b^k$ times $a - b$. And in the case of an integral domain (and $a \neq b$) this even is uniquely determined. And from the explicit representation of the divisor one also finds

$$\frac{f(a)a^k - f(b)b^k}{a-b} \;=\; \sum_{i=0}^{d} f[i] \sum_{j=0}^{k-1+i} a^j b^{k-j} \;\in\; \mathfrak{a}^{k-1}$$

(2.51) Proposition: (viz. 1038)

(i) Let $(R, +, \cdot)$ be any commutative ring then for any a, b and $c \in R$ the relation of divisibility satisfies all of the following properties

$$\begin{aligned} 1 &\mid b \\ a &\mid 0 \\ a &\mid ab \\ 0 \mid b \quad &\Longleftrightarrow \quad b = 0 \\ a \mid 1 \quad &\Longleftrightarrow \quad a \in R^* \\ a \mid b \quad &\Longrightarrow \quad ac \mid bc \end{aligned}$$

(ii) If a, b and $u \in R$ such that $u \in \mathrm{NZD}(R)$ is a non-zero divisor of R, then we find the equivalence of

$$a \mid b \quad \Longleftrightarrow \quad au \mid bu$$

(iii) If $(R, +, \cdot)$ is an integral domain, then *divisibility* is a reflexive, transitive relation that is antisymmetric up to associativity. Formally that is: For any a, b and $c \in R$ we get

$$\begin{aligned} a &\mid a \\ a \mid b \text{ and } b \mid c &\implies a \mid c \\ a \mid b \text{ and } b \mid a &\implies a \approx b \end{aligned}$$

(2.52) Remark:
Let $(R, +, \cdot)$ be a commutative ring, recall that we have defined the set of **relevant** elements of R to be the non-zero, non-units of R, that is

$$R^\bullet \;:=\; R \setminus \left(R^* \cup \{0\}\right)$$

- $R^\bullet = \emptyset$ is empty if and only if $R = 0$ or R is a field.

 Prob if $R = 0$ then trivially $R^\bullet = \emptyset$. Conversely $R^\bullet = \emptyset$ if and only if $R = R^* \cup \{0\}$ or in yet other words, if $R^* = R \setminus \{0\}$. And this is just the definition of R being a field.

- The complement of $R^\bullet$ is multiplicatively closed (which means $1 \notin R^\bullet$ and $a, b \notin R^\bullet \implies ab \notin R^\bullet$)

 $$R \setminus R^\bullet \;=\; R^* \cup \{0\} \text{ is multiplicatively closed}$$

 Prob first of all we have $1 \in R^* \cup \{0\} = R \setminus R^\bullet$ (whether $R = 0$ or not). Now consider $a, b \in R \setminus R^\bullet$. If $a = 0$ or $b = 0$ then $ab = 0$ and hence $ab \in R \setminus R^\bullet$. Else if $a, b \neq 0$ then $a, b \in R^*$ and hence $ab \in R^*$, as the inverse of ab can be given, to be $b^{-1}a^{-1} \in R$.

- If R is an integral domain, then $R^\bullet$ is stable under multiplication with non-zero elements: That is, if $a, r \in R$ with $a \neq 0$ and $r \in R^\bullet$, then we get $ar \in R^\bullet$ again.

 Prob if we had $ar = 0$, then $a = 0$ or $r = 0$, as R is an integral domain. But this is not the case. Suppose $ar \in R^*$, that is $aru = 1$ for some $u \in R$. Then $r(au) = 1$ such that $r \in R^*$ with inverse au. But as $r \in R^\bullet$ this is untrue, as well, such that $ar \in R^\bullet$.

(2.53) Definition:
Let $(R, +, \cdot)$ be a commutative ring and $p \in R$ be an elements of R. Then p is said to be **irreducible** if p is a relevant element of R but cannot be further factored into relevant elements. Formally iff

(1) $p \in R^\bullet$

(2) $\forall\, a, b \in R : \; p = ab \implies a \in R^*$ or $b \in R^*$

Likewise $p \in R$ is said to be a **prime** element of R, iff it is a relevant element of R such that it divides (at least) one of the factors in every product it divides. Formally again, iff

(1) $p \in R^\bullet$

(2) $\forall\, a, b \in R : \; p \mid ab \implies p \mid a$ or $p \mid b$

(2.54) Definition:
Let $(R,+,\cdot)$ be a commutative ring and $a \in R$ and let $\star$ abbreviate either the word *prime* or the word *irreducible*. Then a tupel $(\alpha, p_1, \ldots, p_k)$ (with $k \in \mathbb{N}$ and $k = 0$ allowed!) is said to be a $\star$ **decomposition** of a, iff all of the following three properties are satisfied

(1) $\alpha \in R^*$

(2) $a \;=\; \alpha p_1 \ldots p_k$

(3) $\forall\, i \in 1 \ldots n :\; p_i \in R$ is $\star$

If $(\alpha, p_1, \ldots, p_k)$ at least satisfies (1) and (3) then let us agree to call it a $\star$ **series**. Now any two $\star$ series $(\alpha, p_1, \ldots, p_k)$ and $(\beta, q_1, \ldots, q_l)$ are said to be **essentially equal** [which we will denote by writing $(\alpha, p_1, \ldots, p_k) \approx (\beta, q_1, \ldots, q_l)$], iff they are of the same length, ddeompose the same element and their entries are pairwise associated. Formally $(\alpha, p_1, \ldots, p_k) \approx (\beta, q_1, \ldots, q_l) \;:\Longleftrightarrow$ (1), (2) and (3) where

(1) $k = l$

(2) $\alpha p_1 \ldots p_k \;=\; \beta q_1 \ldots q_l$

(3) $\exists\, \sigma \in S_k :\; \forall\, i \in 1 \ldots k :\; p_i \approx q_{\sigma(i)}$

(2.55) Example: $(\diamondsuit)$
Let $(R,+,\cdot)$ be an integral domain and $a \in R$, then the linear polynomial $p(t) := t - a \in R[t]$ is prime. Note that this need not be true unless R is an integral domain. E.g. for $R = \mathbb{Z}_6$ we have

$$t - 1 = (2t+1)(3t-1) \quad \text{but} \quad t - 1 \not\mid 2t+1,\; t-1 \not\mid 3t-1$$

Prob consider $f, g \in R[t]$ such that $p \mid fg$. that is there is some $h \in R[t]$ such that $(t-a)h = fg$. In particular $f(a)g(a) = (fg)(a) = (a-a)h(a) = 0$. As R is an integral domain this means $f(a) = 0$ or $g(a) = 0$. And from this again we get $p = t - a \mid f$ or $p = t - a \mid g$.

(2.56) Definition:

- Let $(R,+,\cdot)$ be a commutative ring again and $\emptyset \neq A \subseteq R$ be a non-empty subset of R. Then we say that $m \in R$ is a **common multiple** of A, iff every $a \in A$ divides m, formally

$$A \mid m \quad :\Longleftrightarrow \quad \forall\, a \in A \;:\; a \mid m$$

- And thereby m is said to be a **least common multiple** of A, iff m is a common multiple that divides any other common multiple. That is iff m satisfies

 (1) $A \mid m$

 (2) $\forall\, n \in R :\; A \mid n \implies m \mid n$

 And we will denote the set of least common multiples of A by $\operatorname{lcm}(A) := \{\, m \in R \mid (1) \text{ and } (2) \,\}$.

- Analogous to the above we say that an element $d \in R$ is a **common divisor** of A, iff d divides every $a \in A$. We will denote this, by

$$d \mid A \quad :\Longleftrightarrow \quad \forall\, a \in A \,:\, d \mid a$$

- And thereby d is said to be a **greatest common divisor** of A, iff d is a common divisor that is divided by any other common divisor. That is iff d satisfies

 (1) $d \mid A$
 (2) $\forall\, c \in R : c \mid A \implies c \mid d$

 And we will denote the set of greatest common divisors of A by $\gcd(A) := \{\, d \in R \mid (1) \text{ and } (2) \,\}$.

- Finally A is said to **relatively prime**, iff 1 is a greatest common divisor of A. By abuse of notation a finite family of elements $a_1, \ldots, a_k \in R$ is said to be *relatively prime*, iff the set $\{a_1, \ldots, a_k\}$ is relatively prime. By (2.51.(i)) this property can also be formulated, as

$$\begin{aligned} A \text{ relatively prime} \quad &:\Longleftrightarrow \quad 1 \in \gcd(A) \\ &\Longleftrightarrow \quad \forall\, c \in R \;:\; c \mid A \implies c \in R^* \end{aligned}$$

(2.57) Remark: (viz. 1040)

(i) A special case is $A = \{\, a \,\}$ for some $a \in R$. For such a singleton we trivially have $a \in \operatorname{lcm}(A)$ and $a \in \gcd(A)$. And if R is an integral domain then (2.58.(ix)) tells us that thereby

$$\operatorname{lcm}(A) \;=\; \gcd(A) \;=\; aR^*$$

In particular we get $\operatorname{lcm}(1) = \gcd(1) = R^*$ and $\operatorname{lcm}(0) = \gcd(0) = \{0\}$.

(ii) If $A \neq \emptyset$ then picking up 1 does not change the least common multiple and picking up 0 does not change the greatest common divisor

$$\begin{aligned} \operatorname{lcm}\big(A \cup \{\, 1 \,\}\big) &= \operatorname{lcm}(A) \\ \gcd\big(A \cup \{0\}\big) &= \gcd(A) \end{aligned}$$

(iii) In a general commutative ring R for any non-empty subset $A \subseteq R$ we find that $0 \in \gcd(A)$ is equivalent to $A = \{0\}$. In formal terms

$$0 \in \gcd(A) \quad \Longleftrightarrow \quad A = \{0\}$$

And if R is an integral domain and $A \subseteq R$ is non-empty and finite, then $0 \in \operatorname{lcm}(A)$ also is equivalent to to $A = \{0\}$. In formal terms again

$$0 \in \operatorname{lcm}(A) \quad \Longleftrightarrow \quad A = \{0\}$$

(iv) If A is an infinite subset, then $\operatorname{lcm}(A)$ may be zero, as well: As an example consider $R = \mathbb{Z}$ and $A = \mathbb{N}$, then $A \mid k$ is equivalent to $k = 0$ and hence $\operatorname{lcm}(A) = \{0\}$.

(2.58) Proposition: (viz. 1038)

(i) Let $(R,+,\cdot)$ be a commutative ring, $p \in R$ be a prime element and $a_1,\ldots,a_k \in R$ be arbitrary elements of R. Then we obtain the following implication

$$p \mid \prod_{i=1}^{k} a_i \quad \Longrightarrow \quad \exists\, i \in 1\ldots k \,:\, p \mid a_i$$

(ii) Let $(R,+,\cdot)$ be a commutative ring and $p \in R$. Then p is a prime element iff $p \neq 0$ and the principal ideal $pR \trianglelefteq_{\mathrm{i}} R$ is a prime ideal, formally that is

$$p \in R \text{ prime} \quad \Longleftrightarrow \quad p \neq 0 \;\text{ and }\; pR \trianglelefteq_{\mathrm{i}} R \text{ prime}$$

(iii) Let $(R,+,\cdot)$ be a commutative ring, $p \in R$ and $\alpha \in R^*$ a unit of R. Let us again abbreviate the word *prime* or *irreducible* by $\star$, then we have the equivalences of

$$p \text{ is } \star \quad \Longleftrightarrow \quad \alpha p \text{ is } \star$$

(iv) Let $(R,+,\cdot)$ be an integral domain. Then any prime element of R already is irreducible. That is for any $p \in R$ we find the following implication

$$p \text{ is prime} \quad \Longrightarrow \quad p \text{ is irreducible}$$

(v) Let $(R,+,\cdot)$ be an integral domain $0 \neq a \in R$ and $b \in R^\bullet$ be a non-zero non-unit. Then we obtain the following strict inclusion of ideals

$$(ab)R \quad \subset \quad aR$$

(vi) Let $(R,+,\cdot)$ be an integral domain and consider a non-unit $f \in R \setminus R^*$ and a prime element $p \in R$. If f divides p, then f and p already are associates (and vice versa), which is the equivalence

$$f \mid p \quad \Longleftrightarrow \quad f \approx p$$

(vii) Let $(R,+,\cdot)$ be an integral domain, consider some elements $a, b \in R$ and suppose $d \in \gcd\{a,b\}$ is a greatest common divisor of a and b. Then the elements a/d and $b/d \in R$ are relatively prime

$$d \in \gcd\{a,b\} \quad \Longrightarrow \quad 1 \in \gcd\left\{\frac{a}{d}, \frac{b}{d}\right\}$$

(viii) Let $(R,+,\cdot)$ be an integral domain. Then the set D of all $d \in R$ that allow a prime decomposition is saturated and multiplicatively closed. That is $D := \{\alpha p_1 \ldots p_k \mid \alpha \in R^*,\ k \in \mathbb{N},\ p_i \in R \text{ prime}\}$ satisfies the properties

$$\begin{aligned} 1 \quad &\in \quad D \\ c,d \in D \quad &\Longleftrightarrow \quad cd \in D \end{aligned}$$

(ix) Let $(R,+,\cdot)$ be an integral domain and suppose $p_1,\ldots,p_k$ and $q_1,\ldots,q_l \in R$ are finite collections of prime elements of R (where k, $l \in \mathbb{N}$ with $k = 0$ and $l = 0$ allowed) and let α, $\beta \in R^*$ be two units of R. Then the prime decompositions are essentially equal, that is

$$\alpha p_1 \ldots p_k = \beta q_1 \ldots q_l \quad \Longrightarrow \quad \begin{array}{l} k = l \text{ and } \exists\, \sigma \in S_k \text{ such that} \\ \forall\, i \in 1 \ldots k \;:\; p_i \approx q_{\sigma(i)} \end{array}$$

(x) Let $(R,+,\cdot)$ be an integral domain and $\emptyset \neq A \subseteq R$ be a non-empty subset of R. Further let d and $m \in R$ be two elements of R, then we find the equivalences

$$\begin{aligned} m \in \operatorname{lcm}(A) &\iff \operatorname{lcm}(A) = mR^* \\ d \in \gcd(A) &\iff \gcd(A) = dR^* \end{aligned}$$

(2.59) Theorem: (viz. 1041)
Let $(R,+,\cdot)$ be a noetherian integral domain and fix some elements a, b and $p \in R$ where p is prime. Then we obtain the following statements

(i) If $a \in R^\bullet$ then the order in which a divides b is finite. In formal terms we get

$$\langle a \mid b \rangle \;\in\; \mathbb{N}$$

(ii) The order of a prime element $p \in R$ has the properties of a logarithm - it turns multiplications into additions and powers ($n \in \mathbb{N}$) into multiples. That is

$$\begin{aligned} \langle p \mid ab \rangle &= \langle p \mid a \rangle + \langle p \mid b \rangle \\ \langle p \mid a^n \rangle &= n \cdot \langle p \mid a \rangle \end{aligned}$$

(iii) Any $a \neq 0$ admits an irreducible decomposition. That is there are some $\alpha \in R^*$ and finitely many irreducible elements $p_1,\ldots,p_k \in R$ such that a can be written, as

$$a \;=\; \alpha p_1 \ldots p_k$$

(iv) If $0 \neq \mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ is any prime ideal of R then $\mathfrak{p}$ is generated by finitely many irreducible elements. That is there are $p_1,\ldots,p_k \in R$ irreducible, such that

$$\mathfrak{p} \;=\; \langle p_1,\ldots,p_k \rangle_{\mathrm{i}}$$

(v) Let $P \subseteq R^\bullet$ be a set of pairwise non-associate non-zero non-units of R. That is we assume that for any p, $q \in P$ we get $p \approx q \implies p = q$. Then for any $a \neq 0$ the number of $p \in P$ that divide a is finite, formally again we get

$$\#\{\, p \in P \mid a \in pR \,\} \;<\; \infty$$

(vi) Let $b \in R^\bullet$ be a non-zero, non-unit of R. Further consider a finite collection $q_1, \ldots, q_k \in R$ of prime elements of R that are pairwise non-associate. That is we assume $q_i \approx q_j \implies i = j$ for any i, $j \in 1 \ldots k$. Then we obtain the divisibility relation

$$a \;:=\; \prod_{i=1}^{k} q_i^{\langle q_i | b \rangle} \;\Big|\; b$$

In particular, if $q_i \mid b$ for any $i \in 1 \ldots k$ then $q_1 \ldots q_k \mid a$ and hence $q_1 \ldots q_k \mid b$. If now $p \in R$ is any prime element of R, then we obtain another implication

$$p \mid b \quad\Longrightarrow\quad p \mid \frac{b}{a} \quad \text{xor} \quad \exists\, i \in 1 \ldots k : p \approx q_i$$

(2.60) Definition: (viz. 1044)
We call $(R, +, \cdot)$ an **unique factorisation domain** (which we will always abbreviate by **UFD**), iff R is an integral domain that further satisfies one of the following equivalent properties

(a) Every non-zero element admits a decomposition into prime elements. That is for any $0 \neq a \in R$ we get the following statement

$$\exists\ (\alpha, \mathbf{p}) = (\alpha, p_1, \ldots, p_k) \text{ prime decomposition of } a$$

(b) Every non-zero element admits an essentially unique decomposition into irreducible elements. That is for any $a \in R$ with $a \neq 0$ we have

(1) $\exists\, (\alpha, \mathbf{p}) = (\alpha, p_1, \ldots, p_k)$ irreducible decomposition of a

(2) $(\alpha, \mathbf{p}), (\beta, \mathbf{q})$ irreducible decompositions of $a \implies (\alpha, \mathbf{p}) \approx (\beta, \mathbf{q})$

(c) Every non-zero element admits a decomposition into irreducible elements and every irreducible element is prime. Formally these are both of the properties

(1) $\forall\, 0 \neq a \in R\ \ \exists\, (\alpha, \mathbf{p})$ irreducible decomposition of a

(2) $\forall\, p \in R \ :\ p$ prime $\iff p$ irreducible

(d) The principal ideals of R satisfy the ascending chain condition and every irreducible element is prime. Formally these are both of the properties

(1) for any family of elements $a_k \in R$ (where $k \in \mathbb{N}$) of R such that $a_0 R \subseteq a_1 R \subseteq \ldots \subseteq a_k R \subseteq a_{k+1} R \subseteq \ldots$ there is some $s \in \mathbb{N}$ such that for any $i \in \mathbb{N}$ we get $a_{s+i} R = a_s R$.

(2) $\forall\, p \in R \ :\ p$ prime $\iff p$ irreducible

(e) Any non-zero prime ideal of R contains a prime element of R. Let us add a formal version of this:

$$\forall\, \mathfrak{p} \in \operatorname{Spec}(R) \ :\ \mathfrak{p} \neq 0 \quad\Longrightarrow\quad \exists\, p \in R \text{ prime} \ :\ p \in \mathfrak{p}$$

(f) ($\diamondsuit$) Let $D := \{\alpha p_1 \dots p_k \mid \alpha \in R^*,\ k \in \mathbb{N},\ p_i \in R \text{ prime}\}$ denote the set of all elements $d \in R$ that allow a prime decomposition again. Then either $R = 0$ is the zero ring or the quotient field of R is precisely the localization of R in D, formally

$$\text{QUOT}(R) \ = \ D^{-1}R$$

(2.61) Remark:

- The zero-ring $R = 0$ trivially is an UFD. As it does not contain a single non-zero element such that condition (a) of UFDs is void (hence true).
- Property (b) guarantees that - in an UFD $(R, +, \cdot)$ - any nonzero element $0 \neq a \in R$ admits an irreducible (equivalently prime) decomposition $a = \alpha p_1 \dots p_k$, that even is essentially unique. And this uniqueness determines the number k of irreducible factors. Hence we may define the **length** of a to be precisely this number

$$\ell(a) \ := \ k \quad \text{where} \quad (\alpha, p_1, \dots, p_k) \text{ prime decomposition of } a$$

- Any field $(E, +, \cdot)$ is an UFD, as we allowed $k = 0$ for a prime decomposition $(\alpha, p_1, \dots, p_k)$. To be precise if $0 \neq a \in E$ then $a \in E^*$ already is a unit and hence (a) is a prime decomposition of a.
- In the next section we will prove that any PID (i.e. an integral domain in which every ideal can be generated by a single element) is an UFD.
- If $(R, +, \cdot)$ is a noetherian integral domain in which any irreducible element is prime, then R is an UFD. This is clear from property (d) in (2.60).
- If $(R, +, \cdot)$ is an UFD then so is the polynomial ring $R[t]$ (this is the one of the lemmas of Gauss that will be proved in (7.29), all of which are milestones).
- ($\diamondsuit$) If $(R, +, \cdot)$ is an UFD and $U \subseteq R$ is multiplicatively closed, then the localisation $U^{-1}R$ is an UFD too. In fact, if $p \in R$ is a prime element then $p/1$ either is a unit or a prime in $U^{-1}R$. This will be proved in (2.131).
- ($\diamondsuit$) A sub-ring $\mathcal{O} \ \leq_{\mathrm{r}} \ \mathbb{C}$ of the complex numbers is said to be an *algebraic number ring*, iff any $a \in \mathcal{O}$ satisfies an integral equation over $\mathbb{Z}$ (that is there is a monic polynomial $f \in \mathbb{Z}[t]$ such that $f(a) = 0$). We will see that any algebraic number ring $\mathcal{O}$ is a Dedekind domain. And it is also true, that $\mathcal{O}$ is an UFD if and only if it is a PID.
- This list of UFDs is almost exhaustive. At the end of this section we will append a list of counter examples, such that the reader may convince himself that the equivalences in the definition of an UFD cannot be generalized.

(2.62) Remark:
It is often useful not to regard all the prime (resp. irreducible) elements of R but to restrict to a representative set modulo associateness. That is a subset $\mathbb{P} \subseteq R$ such that we have bijection of the form

$$\mathbb{P} \ \longleftrightarrow \ \{\, p \in R \mid p \text{ prime} \,\} \Big/_{\approx} \ : \ p \mapsto pR^*$$

Prob this is possible since $\approx$ is an equivalence relation on R of which the equivalence classes are precisely aR^* by (2.51). In particular $\approx$ also is on equivalence relation on the subset P of prime elements of R. And by (2.58) we know that for any $p \in P$ we have $[p] = \{\, q \in P \mid p \approx q \,\} = pR^*$ again. Hence we may choose $\mathbb{P}$ as a representing system of $P/\approx$ by virtue of the axiom of choice.

(2.63) Example:

- The units of the integers $\mathbb{Z}$ are given to be $\mathbb{Z}^* = \{-1, +1\}$. That is associateness identifies all elements having the same absolute value, $a\mathbb{Z}^* = \{-a, a\}$. And thereby we can choose a representing system of $\mathbb{Z}$ modulo $\approx$ simply by choosing all *positive* elements $a \geq 0$. Thus we find a representing system of the prime elements of $\mathbb{Z}$ by

$$\mathbb{P} \;:=\; \{\, p \in \mathbb{Z} \mid p \text{ prime}, \; 0 \leq p \,\}$$

- ($\diamondsuit$) Now let $(E, +, \cdot)$ be any field and consider the polynomial $E[t]$. Then we will see that the units of $E[t]$ are given to be $E[t]^* = E^* = \{at^0 \mid 0 \neq a \in E\}$. Thus associateness identifies all polynomials having the same coefficients up to a common factor. That is we get $fE[t]^* = \{af \mid 0 \neq a \in E\}$. Thus by requiring a polynomial f to be *normed* (i.e. $f[\deg(f)] = 1$) we eliminate this ambiguity. Therefore we find a representing system of the prime elements of $E[t]$ by

$$\mathbb{P} \;:=\; \{\, p \in E[t] \mid p \text{ prime, normed} \,\}$$

(2.64) Theorem: (viz. 1045)
Let $(R, +, \cdot)$ be an UFD, $p \in R$ be a prime element and $0 \neq a, b \in R$ be any two non-zero elements. Then the following statements hold true

(i) Suppose $(\alpha, p_1, \ldots, p_k)$ is a prime decomposition of a. Then for any prime $p \in R$ the order of p in a can be expressed as the number of appearances of an associate of p in the decomposition:

$$\langle p \mid a \rangle \;=\; \#\{\, i \in 1 \ldots k \mid p \approx p_i \,\} \;\in\; \mathbb{N}$$

(ii) (As in noetherian integral domains) the order of a prime element $p \in R$ has the properties of a logarithm - it turns multiplications into additions and powers ($n \in \mathbb{N}$) into multiples

$$\begin{aligned} \langle p \mid ab \rangle &= \langle p \mid a \rangle + \langle p \mid b \rangle \\ \langle p \mid a^n \rangle &= n \cdot \langle p \mid a \rangle \end{aligned}$$

(iii) We can reformulate divisibility like: a divides b if and only if for any prime p the order of p in a does not exceed the order of p in b. Formally that is the equivalence of

$$a \mid b \quad\Longleftrightarrow\quad \forall\, p \in R \text{ prime} : \langle p \mid a \rangle \leq \langle p \mid b \rangle$$

(iv) If $d \in R$ divides ab but a and d are relatively prime, then d already divides b. Formally that is the following implication

$$d \mid ab \text{ and } 1 \in \gcd\{a, d\} \implies d \mid b$$

(v) Let $\mathbb{P}$ be a representing system of the prime elements modulo associateness. Then for any $0 \neq a \in R$ we obtain a unique representation

$$\exists!\, \alpha \in R^* \;\; \exists!\, n = (n(p)) \in \bigoplus_{p \in \mathbb{P}} \mathbb{N} \;\; : \;\; a = \alpha \prod_{p \in \mathbb{P}} p^{n(p)}$$

and thereby we even have $n(p) = \langle p \mid a \rangle$ such that the sum of all $n(p)$ is precisely the length of a (and in particular finite). Formally that is

$$\ell(a) \;\; = \;\; \sum_{p \in \mathbb{P}} n(p) \;\; < \;\; \infty$$

Nota that $n \in \oplus_p \mathbb{N}$, that is $n : \mathbb{P} \to \mathbb{N}$ is a map such that the number of $p \in \mathbb{P}$ with $n(p) \neq 0$ is finite. And hence the product over all $p^{n(p)}$ (where $p \in \mathbb{P}$) well-defined using the notations of section 1.3.

(vi) Let $\mathbb{P}$ be a representing system of the prime elements modulo associateness again. And consider a non-empty subset $\emptyset \neq A \subseteq R$ such that $0 \notin A$. Then A has a greatest common divisor, namely

$$\prod_{p \in \mathbb{P}} p^{m(p)} \in \gcd(A) \quad \text{where} \quad m(p) := \min\{\, \langle p \mid a \rangle \mid a \in A \,\}$$

Likewise if $A = \{a_1, \ldots, a_n\} \subseteq R$ is a non-empty, finite ($1 \leq n \in \mathbb{N}$) subset with $0 \notin A$ then A has a least common multiple, namely

$$\prod_{p \in \mathbb{P}} p^{n(p)} \in \operatorname{lcm}(A) \quad \text{where} \quad n(p) := \max\{\, \langle p \mid a \rangle \mid a \in A \,\}$$

(vii) Let $A := \{\, a, b \,\}$ and $d \in \gcd(A)$ be a greatest common divisor, $m \in \operatorname{lcm}(A)$ a least common multiple of a and b. Then we obtain

$$ab \;\; \approx \;\; dm$$

(vii) If $0 \neq a, b, c \in R$ are any three non-zero elements of R, then the least common multiple and greatest common divisor of these can be evaluated recursively. That is if $d \in \gcd\{a, b\}$ and $m \in \operatorname{lcm}\{a, b\}$ then we get the recursion formuale

$$\begin{aligned} \gcd\{\, a, b, c \,\} &= \gcd\{\, d, c \,\} \\ \operatorname{lcm}\{\, a, b, c \,\} &= \operatorname{lcm}\{\, m, c \,\} \end{aligned}$$

(2.65) Proposition: (viz. 1047) ($\diamondsuit$)
Any UFD R is a normal domain. Thereby a commutative ring $(R, +, \cdot)$ is said to be *normal* (or *integrally closed*), iff R is integrally closed in its total ring of fractions. That is R is a **normal domain**, iff it satisfies the following two properties:

(1) R is an integral domain

(2) R is **normal**, that is: For any a, $b \in R$ with $a \neq 0$ we get: If there is some monic polynomial $f \in R[t]$ such that $f(b/a) = 0 \in \mathrm{QUOT}(R)$, then we already had $a \mid b$.

(2.66) Example: (viz. 1048)

(i) *UFDs need not be noetherian!* As an example regard a field $(E, +, \cdot)$, then the polynomial ring in countably many variables $E[t_i \mid i \in \mathbb{N}]$ is an UFD by the lemma of Gauss (7.29). But it is not noetherian (by the examples in section 2.4).

(ii) *Noetherian integral domains need not be UFDs!* As an example we would like to present the following algebraic number ring

$$\mathbb{Z}[\sqrt{-3}] \;:=\; \left\{ a + ib\sqrt{3} \mid a, b \in \mathbb{Z} \right\} \;\subseteq\; \mathbb{C}$$

It is quite easy to see that in this ring $2 \in \mathbb{Z}[\sqrt{-3}]$ is an irreducible element, that is not prime. Hence $\mathbb{Z}[\sqrt{-3}]$ cannot be an UFD. Never the less it is an integral domain (being a sub-ring of $\mathbb{C}$) and noetherian (by Hilbert's basis theorem (2.42), as it is generated by $\sqrt{-3}$ over $\mathbb{Z}$).

(iii) *Residue rings (even integral domains) of UFDs need not be UFDs!* As an example let us start with the polynomial ring $\mathbb{R}[s, t]$ in two variables over the reals. Then $\mathbb{R}[s, t]$ is an UFD by the lemma of Gauss (7.29). Now consider the residue ring

$$R \;:=\; \mathbb{R}[s,t] \Big/ \mathfrak{p} \quad \text{where} \quad \mathfrak{p} \;:=\; (s^2 + t^2 - 1)\mathbb{R}[s,t]$$

Then $p(s, t) = s^2 + t^2 - 1 \in \mathbb{R}[s, t]$ is an irreducible (hence prime) polynomial, such that $\mathfrak{p}$ is a prime ideal. Yet we are able to prove that R is not an UFD (in fact we will prove that there is an irreducible, non-prime element in a certain localization of R).

2.6 Euclidean Domains

For now we have studied the internal structure of rings. But if we take a look at polynomial ring (we have introduced the easiest, but most important case in (1.33)) we see that these feature the degree as an external function that neatly defines the structure of the ring. The most noteworthy property of polynomials is division with remainder. We already encountered this with the integers $\mathbb{Z}$, as well. In this case the external function is the absolute value. So it seems worthwhile to study these external functions and their impact on the ring's internal structure in general. As an instructive example let us stick to the polynomials first:

(2.67) Lemma: (viz. 747)
Let $(R, +, \cdot)$ be any commutative ring and fix a monic polynomial $f \in R[t]$ (i.e. $\mathrm{lc}(f) = 1$) over R. Then for any other polynomial $g \in R[t]$ there are q, $r \in R[t]$ such that the following two properties hold true

(1) $g = qf + r$

(2) $\deg(r) < \deg(f)$ or $r = 0$

If R is an integral domain, then these polynomials q and r are uniquely determined and it is customary to introduce two binary operations, to denote them

$$\begin{aligned} g \text{ div } f &:= q \\ g \text{ mod } f &:= r \end{aligned}$$

(2.68) Remark:
The proof of the above lemma even provides an algorithm (that we present in *pseudo-code* here) how to iteratively compute these polynomials q and r

input	$f \in R[t]$ monic,
	$g \in R[t]$
initialisation	$q \leftarrow 0$
	$r \leftarrow g$
	$m \leftarrow \deg(f)$
algorithm	while $r \neq 0$ and $\deg(r) \geq \deg(f)$ do begin
	$\quad n \leftarrow \deg(r)$
	$\quad p \leftarrow q + \mathrm{lc}(r)\, t^{n-m}$
	$\quad q \leftarrow q + p$
	$\quad r \leftarrow r - p \cdot f$
	end-while
output	q, r

Let us take the division with remainder property of polynomials as a pattern how to generally define what a division with remainder should provide. As an ingredient we need an external function $\nu = \deg$ that gives a criterion whether the remainder r is smaller than the dividend f.

(2.69) Definition:
Let $(R,+,\cdot)$ be an integral domain and ν be a mapping of the form $\nu : R \setminus \{0\} \to \mathbb{N}$. Then the ordered pair (R,ν) is said to be an **Euclidean domain**, iff R allows *division with remainder* - that is for any a and $b \in R$ with $a \neq 0$ there are q, $r \in R$ such that we get

(1) $b = qa + r$

(2) $\nu(r) < \nu(a)$ or $r = 0$

(2.70) Remark:

- In this general setting the division with remainder need *not* be unique. Even in case $R = \mathbb{Z}$ of the integers we have $7 = 3 \cdot 2 + 1$ but also $7 = 4 \cdot 2 - 1$. It does get uniquely determined once we impose the additional condition $r \geq 0$, as we have seen in (1.28). However we will sometimes want to address these elements q and $r \in R$, even if there is no deterministic function to do so. Hence q is said to be the *quotient* and r is said to be the *remainder* of this operation. And we occasionally dare to employ the following notation, even if it suggests a functional correspondence that does not exist in the general setting!

$$\begin{aligned} b \text{ div } a &:= q \\ b \text{ mod } a &:= r \end{aligned}$$

- We will employ a notational trick to eliminate the distinction of the case $r = 0$ in the definition above. To do this we pick up a symbol $-\infty$ and set $-\infty < n$ for any $n \in \mathbb{N}$. Then we extend ν to

$$\nu \; : \; R \to \mathbb{N} \cup \{-\infty\} \; : \; a \mapsto \begin{cases} \nu(a) \text{ if } a \neq 0 \\ -\infty \text{ if } a = 0 \end{cases}$$

 Thereby the property to allow division with remainder simply reads as: For any a, $b \in R$ with $a \neq 0$ there are q, $r \in R$ such that we get both of the properties

 (1) $b = qa + r$
 (2) $\nu(r) < \nu(a)$

- In an Euclidean domain (R,ν) any $a \in R$ that satisfies $\nu(a) = 0$ already is a unit $a \in R^*$ of R. The converse need not be true however. That is we have the inclusion (but not necessarily equality)

$$\{\, a \in R \mid \nu(a) = 0 \,\} \quad \subseteq \quad R^*$$

 Prob using division with remainder we find q, $r \in R$ such that $1 = qa + r$ and $\nu(r) < \nu(a) = 0$. But the latter means $\nu(r) = -\infty$ and hence $r = 0$. We are left with $1 = qa$ and hence $a \in R^*$.

(2.71) Example: (viz. 1050)

(i) If $(E,+,\cdot)$ is a field, then (E,ν) is an Euclidean domain under any function $\nu : E \setminus \{0\} \to \mathbb{N}$. Because for any $0 \neq a \in E$ and $b \in E$ we may let $q := ba^{-1}$ and $r := 0$.

(ii) The ring $\mathbb{Z}$ of integers is an Euclidean domain $(\mathbb{Z}, \alpha)$ under the (slightly modified) absolute value α as an Euclidean function

$$\alpha \ : \ \mathbb{Z} \to \mathbb{N} \cup \{ -\infty \} \ : \ a \mapsto \begin{cases} a \text{ if } a > 0 \\ -a \text{ if } a < 0 \\ -\infty \text{ if } a = 0 \end{cases}$$

In fact consider $1 \leq a \in \mathbb{Z}$ and any $b \in \mathbb{Z}$ then for $q := b \text{ div } a$ and $r := b \bmod a$ (see below for a definition) we have $b = aq + r$ and $0 \leq r < a$ (in particular $\alpha(r) < \alpha(a)$). And in case $a < 0$ we can choose q and r similarly to have division with remainder.

$$\begin{aligned} b \text{ div } a &:= \max\{ q \in \mathbb{Z} \mid aq \leq b \} \\ b \bmod a &:= b - (b \text{ div } a) \cdot a \end{aligned}$$

(iii) If $(E, +, \cdot)$ is a field then the polynomial ring $E[t]$ in one variable over E is an Euclidean domain $(E[t], \deg)$ under the *degree* function

$$\deg \ : \ E[t] \setminus \{0\} \ : \ f \mapsto \max\{ k \in \mathbb{N} \mid f[k] \neq 0 \}$$

This is true because of the division algorithm for polynomials - see (2.67). Note that the division algorithm can be applied, as any non-zero polynomial can be made monic, since E is a field. However $R[t]$ will not be a Euclidean ring, unless R is a field. Also, though the division algorithm for polynomials can be generalized to Buchberger's algorithm, it is *untrue* that the polynomial ring $E[t_1, \ldots, t_n]$ is an Euclidean domain (for $n \geq 2$) under some Euclidean function ν.

(iv) Consider any $d \in \mathbb{Z}$ that is not the square of another integer, that is $\sqrt{d} \notin \mathbb{Z}$. Then we consider the sub-ring of $\mathbb{C}$ generated by $\sqrt{d}$

$$\mathbb{Z}[\sqrt{d}] \ := \ \left\{ a + b\sqrt{d} \mid a, b \in \mathbb{Z} \right\} \ \subseteq \ \mathbb{C}$$

Then the representation $x = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ is unique (that is for any a, b, f and $g \in \mathbb{Z}$ we get $a + b\sqrt{d} = f + g\sqrt{d} \iff (a, b) = (f, g)$). And thereby we obtain a well-defined ring-automorphism on $\mathbb{Z}[\sqrt{d}]$ by virtue of $x = a + b\sqrt{d} \mapsto \overline{x} := a - b\sqrt{d}$. Now define

$$\nu \ : \ \mathbb{Z}[\sqrt{d}] \setminus \{0\} \to \mathbb{N} \ : \ x = a + b\sqrt{d} \mapsto |x\overline{x}| = |a^2 - db^2|$$

Then ν is multiplicative, that is $\nu(xy) = \nu(x)\nu(y)$ for any x, $y \in \mathbb{Z}[\sqrt{d}]$. And it is quite easy to see that the units of $\mathbb{Z}[\sqrt{d}]$ is given to be

$$\mathbb{Z}[\sqrt{d}]^* \ = \ \left\{ x \in \mathbb{Z}[\sqrt{d}] \ \middle| \ \nu(x) = 1 \right\}$$

We will prove that for $d \leq -3$ the ring $\mathbb{Z}[\sqrt{d}]$ will not be an UFD, as 2 is an irreducible element, that is not prime. Yet for $d \in \{-2, -1, 2, 3\}$, we find that $(\mathbb{Z}[\sqrt{d}], \nu)$ is an Euclidean domain.

(2.72) Proposition: (viz. 1052)
Let (R,ν) be an Euclidean domain and $0 \neq a, b \in R$ be two non-zero elements. Then a and b have a greatest common divisor $g \in R$ that can be computed by the following (so called *Euclidean*) *algorithm*

input	$0 \neq a, b \in R$
initialisation	if $\nu(a) \leq \nu(b)$
	then $(f \leftarrow a, g \leftarrow b)$
	else $(f \leftarrow b, g \leftarrow a)$
algorithm	while $f \neq 0$ do begin
	choose $q, r \in R$ with
	$(g = qf + r$ and $\nu(r) < \nu(f))$
	$g \leftarrow f, f \leftarrow r$
	end-while
output	g

That is given $0 \neq a, b \in R$ we start the above algorithm that returns $g \in R$ and for this g we get $g \in \gcd\{a,b\}$. If now g denotes the greatest common divisor $g \in \gcd\{a,b\}$ of a and b, then there are r and $s \in R$ such that $g = ra + sb$. And these r and s can be computed (along with g) using the following enhancement of the *Euclidean algorithm*

input	$0 \neq a, b \in R$
initialisation	if $\nu(a) \leq \nu(b)$
	then $(f_1 \leftarrow b, f_2 \leftarrow a)$
	else $(f_1 \leftarrow a, f_2 \leftarrow b)$
algorithm	$k \leftarrow 1$
	repeat
	$k \leftarrow k + 1$
	choose q_k and $f_{k+1} \in R$ with
	$(f_{k-1} = q_k f_k + f_{k+1}$
	and $\nu(f_{k+1}) < \nu(f_k))$
	until $f_{k+1} = 0$
	$n \leftarrow k, g \leftarrow f_n$
	$r_2 \leftarrow 1, s_2 \leftarrow 0$
	$r_3 \leftarrow -q_2, s_3 \leftarrow 1$
	for $k = 3$ to $n-1$ step 1 do begin
	$r_{k+1} \leftarrow r_{k-1} - q_k r_k$
	$s_{k+1} \leftarrow s_{k-1} - q_k s_k$
	end-for
	if $\nu(a) \leq \nu(b)$
	then $(r \leftarrow r_n, s \leftarrow s_n)$
	else $(r \leftarrow s_n, s \leftarrow r_n)$
output	g, r and s

(2.73) Remark: $(\diamondsuit)$
In the case of $R = \mathbb{Z}$ it is well-known, that the units of $\mathbb{Z}_a = \mathbb{Z}/a\mathbb{Z}$ are precisely those $b + a\mathbb{Z}$ that satisfy $\gcd(a, b) = \pm 1$. And thereby the enhanced Euclidean algorithm even provides an efficient way of finding the inverse of $b + a\mathbb{Z}$. Use the algorithm to obtain r and $s \in \mathbb{Z}$ such that $1 = g = ra + sb$, then $1 + a\mathbb{Z} = (bs + a\mathbb{Z}) = (b + a\mathbb{Z})(s + a\mathbb{Z})$. Hence $s + a\mathbb{Z}$ is the inverse of $b + a\mathbb{Z}$. This is not purely theoretic, this computation is part of the RSA algorithm.

(2.74) Remark:
Presented in pseudo-code (as we did here) the Euclidean algorithm may seem a little artificial, but the idea behind it is quite simple: Given a and $b \in R$ we first look for a greatest common divisor g of a and b. First we arrange a and b in ascending order, that is we let $\{ f_1, f_2 \} = \{ a, b \}$ such that $\nu(f_2) \leq \nu(f_1)$. Then we use division with remainder successively, denoting $q_k := f_{k-1} \text{ div } f_k$ and $f_{k+1} := f_{k-1} \bmod f_k$. That is the next f_{k+1} is the remainder under the division of f_{k-1} by f_k. Hence we get a sequel of equations

$$\begin{aligned} f_1 &= q_2 f_2 + f_3 \\ f_2 &= q_3 f_3 + f_4 \\ &\vdots \\ f_{n-2} &= q_{n-1} f_{n-1} + f_n \\ f_{n-1} &= q_n f_n + 0 \end{aligned}$$

The thing is that at some point $n \in \mathbb{N}$ we find the remainder $f_{n+1} = 0$, that is f_n divides f_{n-1}. Once we have arrived here $g := f_n$ is a greatest common divisor of a and b. In other words: The greatest common divisor of a and b is the last non-zero remainder f_n in this chain of divisions with remainder.
But the enhanced Euclidean algorithm yields even more: Some r and $s \in R$ such that $g = ra + sb$. And the idea to find these coefficients r and s is quite simple again: Solve the above equations for the respective remainders, that is we compute

$$\begin{aligned} f_3 &= f_1 - q_2 f_2 \\ f_4 &= f_2 - q_3 f_3 \\ f_5 &= f_3 - q_4 f_4 \\ &\vdots \\ f_n &= f_{n-2} - q_{n-1} f_{n-1} \end{aligned}$$

Then we may replace f_3 in the equation for f_4 using the equation beforehand. This results in the equation $f_4 = f_2 - q_3(f_1 - q_2 f_2) = (1 + q_2)f_2 - q_3 f_1$. Now f_3 and f_4 appear in the equation for f_5 again. Replacing both with the previous two equations we find $f_5 = (f_1 - q_2 f_2) - q_4((1 + q_2)f_2 - q_3 f_1) = (1 + q_3 q_4)f_1 - (q_2 + q_4 + q_2 q_4)f_2$. Continuing like this we finally arrive at some equation of the form $f_n = \square f_1 + \square f_2$. And as $g = f_n$ is the greatest common divisor and f_1 and f_2 are just a and b this is precisely what we sought.

All this can be summarized in the following table: Let us assume $v(a) \leq v(b)$ and recall the notation $b \text{ div } a := q$ and $b \text{ mod } a := r$ where q and $r \in R$ are some (not uniquely determined) elements such that $b = qa + r$ and $v(r) < v(a)$. Then we can compute a greates common divisor $g \in \gcd(a, b)$

k	f_{k-1}	f_k	f_{k+1}	q_k
2	b	a	$b \text{ mod } a$	$b \text{ div } a$
3	a	$b \text{ mod } a$	$*$	$*$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
k	f_{k-1}	f_k	$f_{k-1} \text{ mod } f_k$	$f_{k-1} \text{ div } f_k$
k+1	f_k	f_{k+1}	$f_k \text{ mod } f_{k+1}$	$f_k \text{ div } f_{k+1}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
n-1	f_{n-2}	f_{n-1}	g	$*$
n	f_{n-1}	g	0	f_{n-1}/g

The expanded Euclidean algorithm appends this table by the columns r_k and s_k in order to compute the elements $r, s \in R$ such that $g = ra + sb$

k	q_k	r_k	s_k
2	$b \text{ div } a$	1	0
3	$*$	$-(b \text{ div } a)$	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$
k	$f_{k-1} \text{ div } f_k$	$r_{k-2} - q_{k-1}r_{k-1}$	$s_{k-2} - q_{k-1}s_{k-1}$
k+1	$f_k \text{ div } f_{k+1}$	$r_{k-1} - q_k r_k$	$r_{k-1} - q_k r_k$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
n	f_{n-1}/g	r	s

(2.75) Example:
As an application we want to compute the greatest common divisor of $a = 84$ and $b = 1330$ in $\mathbb{Z}$. That is we initialize the algorithm with $f_1 := b = 1330$ and $f_2 := a = 84$. Then we find $1330 = 15 \cdot 84 + 70$ (at $k = 2$), which is $q_2 = 15$ and $f_3 = 70$. Thus in the next step (now $k = 3$) we observe $84 = 1 \cdot 70 + 14$, that is we may choose $q_3 := 1$ and $f_4 := 14$. Now (at counter $k = 4$) we have $70 = 5 \cdot 14 + 0$ which means $q_4 = 5$ and $f_5 = 0$. Thus for $n := k = 4$ we have finally arrived at $f_{k+1} = 0$ terminating the first part of the algorithm. It returns $g = f_n = 14$ the greatest common divisor of $a = 84$ and $b = 1330$. The following table summarizes the computations

k	f_{k-1}	f_k	f_{k+1}	q_k
2	1330	84	70	15
3	84	70	14	1
4	70	14	0	5

Now in the second part of the algorithm we initialize $r_2 := 1$, $s_2 := 0$, $r_3 := -q_2 = -15$ and $s_3 := 1$. Then we compute $r_4 := r_2 - q_3 r_3 = 16$ and $s_4 := s_2 - q_3 s_3 = -1$. As $n = 4$ this already is $r = r_4 = 16$ and $s = s_4 = -1$. And in fact $ra + bs = 14 = g$. Again we summarize these computations in

k	q_k	r_k	s_k
2	15	1	0
3	1	-15	1
4	5	16	-1

(2.76) Proposition: (viz. 1053)
Consider an integral domain $(R,+,\cdot)$ and let $n \in \mathbb{N}$, then we recursively define a subset R_n of n-th level elements of R. The 0-th level elements are the units of R. The $(n+1)$-th level elements are those $a \in R$, that divide all $b \in R$ up to some n-th level element $r \in R_n$. Formally that is

$$\begin{aligned} R_0 &:= R^* = \{\, a \in R \mid \exists\, b \in R : ab = 1 \,\} \\ R_{n+1} &:= \{\, a \in R \setminus \{0\} \mid \forall\, b \in R\ \exists\, r \in R_n \cup \{0\} : a \mid b - r \,\} \end{aligned}$$

(i) The subsets $R_n \subseteq R$ form an ascending chain $R_0 \subseteq R_1 \subseteq \ldots \subseteq R_n \subseteq R_{n-1} \subseteq \ldots$

(ii) If (R,ν) is an Euclidean domain that for any $n \in \mathbb{N}$ the set of $a \in R$ with $a \neq 0$ and $\nu(a) \leq n$ is contained in R_n, formally that is the inclusion

$$\{\, a \in R \mid \nu(a) \leq n \,\} \subseteq R_n \cup \{0\}$$

(iii) Conversely if the R_n cover R, that is $R \setminus \{0\} = \bigcup_n R_n$, then (R,μ) becomes an Euclidean domain under the following Euclidean function

$$\mu : R \setminus \{0\} : a \mapsto \min\{\, n \in \mathbb{N} \mid a \in R_n \,\}$$

And thereby μ satisfies the following two statements for any $a, b \in R$ where $b \neq 0$

$$\mu(a) \leq \mu(ab)$$

$$\mu(b) = \mu(ab) \iff a \in R^*$$

(iv) In particular R is an Euclidean domain, if and only if these sets R_n cover $R \setminus \{0\}$. Put formally

$$R \setminus \{0\} = \bigcup_{n \in \mathbb{N}} R_n \iff \exists\, \nu : (R,\nu) \text{ Euclidean domain}$$

(v) If (R,ν) is an Euclidean domain, then (R,μ) is an Euclidean domain, too and for any $a \in R$ we get $\mu(a) \leq \nu(a)$. In this sense μ is the *minimal Euclidean function* on R.

2.7 Principal Ideal Domains

(2.77) Definition:
Let $(R,+,\cdot)$ be any commutative ring, then an ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ is said to be **principal**, iff it can be generated by a single element, i.e. $\mathfrak{a} = aR$ for some $a \in R$. And R is said to be a **principal ring** iff every ideal of R is principal, that is iff

$$\forall\, \mathfrak{a} \trianglelefteq_{\mathrm{i}} R \;\; \exists\, a \in R \;\; : \;\; \mathfrak{a} = aR$$

Finally R is said to be a **principal ideal domain** (which we will always abbreviate by **PID**), iff it is an integral domain in which every ideal is generated by a single element:

(1) R is an integral domain and

(2) $\forall\, \mathfrak{a} \trianglelefteq_{\mathrm{i}} R\; \exists\, a \in R \;:\; \mathfrak{a} = aR$

(2.78) Remark:

- Clearly the trivial ideals $\mathfrak{a} = 0$ and $\mathfrak{a} = R$ always are principal, as they can be generated by the elements $0 = 0R$ and $R = 1R$ respectively.
- If R is a principal ring and $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ is any ideal, then the quotient ring $R/\mathfrak{a}$ is principal, too. Prob due to the correspondence theorem (1.66) any ideal $\mathfrak{u} \trianglelefteq_{\mathrm{i}} R/\mathfrak{a}$ is of the form $\mathfrak{u} = \mathfrak{b}/\mathfrak{a}$ for some ideal $\mathfrak{a} \subseteq \mathfrak{b} \trianglelefteq_{\mathrm{i}} R$. Thus there is some $b \in R$ with $\mathfrak{b} = bR$. Now let $u := b + \mathfrak{a}$, then clearly $\mathfrak{u} = \{\, bh + \mathfrak{a} \mid h \in R \,\} = u(R/\mathfrak{a})$ is a principal ideal, too.
- Let $R_1, \ldots, R_n$ be principal rings, then the direct sum $R_1 \oplus \cdots \oplus R_n$ is a principal ring, too. Prob by (1.97) the ideals of the direct sum are of the form $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n$ for some ideals $\mathfrak{a}_i \trianglelefteq_{\mathrm{i}} R_i$. Thus by assumption there are some $a_i \in R_i$ such that $\mathfrak{a}_i = a_i R_i$. And thereby it is clear, that $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n = (a_1, \ldots, a_n)R_1 \oplus \cdots \oplus R_n$ is principal again.

(2.79) Lemma: (viz. 1054)

(i) If $(R,+,\cdot)$ is a PID (in particular non-zero), then all non-zero prime ideals of R already are maximal, formally (in a fancier language this can be put as $\mathrm{kdim} R \leq 1$). That is

$$\mathrm{Spec}(R) \;\; = \;\; \mathrm{Smax}(R) \cup \{0\}$$

(ii) If $(R,+,\cdot)$ is a PID then R already is a noetherian ring and an UFD. That is any $0 \neq a \in R$ admits an (essentially uniqe) decomposition $a = \alpha p_1 \ldots p_k$ into prime elements p_i - viz. (2.60).

(iii) If (R,ν) is an Euclidean domain then R already is a PID. In fact if $0 \neq \mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ is a non-zero ideal then $\mathfrak{a} = aR$ for any $a \in \mathfrak{a}$ satisfying

$$\nu(a) \;\; = \;\; \min\{\, \nu(b) \mid 0 \neq b \in \mathfrak{a} \,\}$$

(iv) If $(R,+,\cdot)$ is an integral domain such that any prime ideal is principal, then R already is a PID. Put formally that is the equivalence of the statements

$$R \text{ PID} \;\; \Longleftrightarrow \;\; \forall\, \mathfrak{p} \in \mathrm{Spec}(R) \;\; \exists\, p \in R \;:\; \mathfrak{p} = pR$$

(2.80) Proposition: (viz. 1055)
Let $(F,+,\cdot)$ be any (even a finite) field, then for any $1 \leq n \in \mathbb{N}$ the polynomial ring $F[t_1,\ldots,t_n]$ in finitely many variables over F has infinitely many maximal ideals. In terms of the sprectrum

$$\#\mathrm{Smax}\big(F[t_1,\ldots,t_n]\big) \;=\; \infty$$

(2.81) Remark:

- In (2.71.(i)) we have seen that any field E is an Euclidean domain (under any ν). Hence any field is a PID due to (iii) above. But this is also clear from the fact that the only ideals of a field E are 0 and E itself. And these are principal due to $0 = 0E$ and $E = 1E$. Also (i) is trivially satisfied: The one and only prime ideal of a field is 0.

- The items (i) and (ii) in the above lemma are very useful and will yield a multitude of corollaries (e.g. the lemma of Kronecker that gives birth to field theory). And (iii) provides one of the reasons why we have introduced Euclidean domains: Combining (iii) and (ii) we see that any Euclidean domain is an UFD. And this yields an elegant way of proving that a certain integral domain R is an UFD. Just establish an Euclidean function ν on R and voilà R is an UFD.

- Due to example (2.71.(ii)) we know that $(\mathbb{Z},\alpha)$ is an Euclidean domain. By (iii) above this means that $\mathbb{Z}$ is a PID and (ii) then implies that $\mathbb{Z}$ is an UFD. By definition of UFDs this means that $\mathbb{Z}$ allows essentially unique prime decomposition. This now is a classical result that is known as the *Fundamental Theorem of Arithmetic*. We have proved an even stronger version, namely

$$(R,\nu) \text{ Euclidean domain} \quad\Longrightarrow\quad R \text{ is an UFD}$$

- In the subsequent proposition we will discuss how far a PID deviates from being an Euclidean domain (though this is of little practical value). To do this we will introduce the notion of a Dedekind-Hasse norm. We will then see that an Euclidean function can be easily turned into a Dedekind-Hasse norm and that R is a PID if and only if it admits a Dedekind-Hasse norm. This of course is another way of proving that any Euclidean domain is a PID.

(2.82) Proposition: (viz. 1056)

(i) If $(R,+,\cdot)$ is a PID then R admits a multiplicative *Dedekind-Hasse* norm. That is there is a function $\delta : R \to \mathbb{N}$ satisfying the following three properties for any $a, b \in R$

(1) $\delta(ab) \;=\; \delta(a)\delta(b)$

(2) $\delta(a) = 0 \iff a = 0$

(3) if $a, b \neq 0$ then $b \in aR$ or $\exists\, r \in aR + bR$ such that $\delta(r) < \delta(a)$

Nota to be precise we may define $\delta(0) := 0$ and for any $0 \neq a \in R$ we let $\delta(a) := 2^k$ for $k := \ell(a)$ the length of any decomposition of $a = \alpha p_1 \ldots p_k$ into prime elements.

(ii) If $(R,+,\cdot)$ is an integral domain and δ is a Dedekind-Hasse norm on R (that is $\delta : R \to \mathbb{N}$ is a function satisfying (2) and (3) in (i)), then R already is a PID. In fact if $0 \neq \mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$ is a non-zero ideal then we get $\mathfrak{a} = aR$ for any $0 \neq a \in \mathfrak{a}$ satisfying

$$\delta(a) \quad = \quad \min\{\, \delta(b) \mid 0 \neq b \in \mathfrak{a} \,\}$$

(iii) If (R,ν) is an Euclidean domain then we obtain a Dedekind-Hasse norm on R (that is $\delta : R \to \mathbb{N}$ satisfies (2) and (3) in (i)) by letting

$$\delta \;:\; R \to \mathbb{N} \;:\; a \mapsto \begin{cases} 0 \text{ if } a = 0 \\ \nu(a) + 1 \text{ if } a \neq 0 \end{cases}$$

(2.83) Lemma: (viz. 1056) **of Bezout**
Let $(R,+,\cdot)$ be an integral domain and $A \subseteq R$ be a non-empty $A \neq \emptyset$ subset of R. Then we obtain the following statements

(i) The intersection of the ideals aR (where $a \in A$) is a principal ideal if and only if A admits a least common multiple. More precisely for any $m \in R$ we obtain the following equivalence

$$\bigcap_{a \in A} aR = mR \quad \Longleftrightarrow \quad m \in \operatorname{lcm}(A)$$

(ii) If the sum of the ideals aR (where $a \in A$) is a principal ideal then A admits a greatest common divisor. More precisely for any $d \in R$ we obtain the following equivalence

$$\sum_{a \in A} aR = dR \quad \Longrightarrow \quad d \in \gcd(A)$$

Nota the converse implication is *untrue* in general. E.g. regard the polynomial ring $R = \mathbb{Z}[t]$, then $1 \in \gcd(2,t)$ but the ideal $2R + tR$ is not principal. The converse is true in PIDs however:

(iii) If R even is a PID then the sum of the ideals aR (where $a \in A$) is the principal ideal generated by the greatest common divisor of A. More precisely for any $d \in R$ we obtain the following equivalence

$$\sum_{a \in A} aR = dR \quad \Longleftrightarrow \quad d \in \gcd(A)$$

In particular in a PID a greatest common divisor $d \in \gcd(A)$ can be written as a linear combination of elements of $a \in A$, formally this is the property

$$\exists\, (b_a) \in R^{\oplus A} \;\; : \;\; d \;=\; \sum_{a \in A} a b_a$$

Nota in an Euclidean ring (R,ν) (supposed that A is finite) the Euclidean algorithm (2.72) provides an effective method to (recursively, using (2.64.(viii))) compute these elements b_a.

(iv) Let R be a PID again and consider finitely many non-zero elements $0 \neq a_1, \ldots, a_n \in R$ such that the a_i are pairwise relatively prime (that is $i \neq j \in 1 \ldots n \implies 1 \in \gcd(a_i, a_j)$). If now $b \in R$ then there are $b_1, \ldots, b_n \in R$ such that we obtain the equality (in the quotient field $\mathrm{QUOT}(R)$ of R)

$$\frac{b}{a_1 \ldots a_n} = \frac{b_1}{a_1} + \cdots + \frac{b_n}{a_n}$$

In an UFD R any collection $A \subseteq R$, $A \neq \emptyset$ of elements of R has a greatest common divisor d, due to (2.64.(v)). And we have just seen that in a PID the greatest common divisor d, that can even be written as a linear combination $d = \sum_a ab_a$. In an Euclidean domain d and the b_a can even be computed algorithmically, using the Euclidean algorithm. We now ask for the converse, that is: If any finite collection of elements of R has a greatest common divisor, that is a linear combination of the collection, can we then conclude that R a PID already? The answer will be *yes* for noetherian rings, but *no* in general.

(2.84) Definition: (viz. 1057)
Let $(R, +, \cdot)$ be an integral domain, then R is said do be a **Bezout domain** iff it satisfies one of the following three equivalent properties

(a) Any two elements a, $b \in R$ admit a greatest common divisor, that can be written as a linear combination of a and b. Formally that is

$$\forall\, a, b \in R \;\; \exists\, r, s \in R \;\; : \;\; ra + sb \in \gcd\{a, b\}$$

(b) For any a, $b \in R$ the ideal $aR + bR$ is principal, that is there is some $d \in R$ such that we get $dR = aR + bR$. Formally again that is

$$\forall\, a, b \in R \;\; \exists\, d \in R \;\; : \;\; dR = aR + bR$$

(c) Any finitely generated ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ of R is principal. We write this as a formal implication again:

$$\forall\, \mathfrak{a} \trianglelefteq_{\mathrm{i}} R \;\; : \;\; \mathfrak{a} \text{ finitely generated} \implies \mathfrak{a} \text{ principal}$$

(2.85) Corollary: (viz. 1058)
Let $(R, +, \cdot)$ be any ring ring, then the following statements are equivalent

(a) R is a PID

(b) R is an UFD and Bezout domain

(c) R is a noetherian ring and Bezout domain

(2.86) Example:

(i) Let $R := \mathbb{Z} + t\mathbb{Q}[t] := \{f \in \mathbb{Q}[t] \mid f(0) \in \mathbb{Z}\} \subseteq \mathbb{Q}[t]$ be the sub-ring of polynomials over $\mathbb{Q}$ with constant term in $\mathbb{Z}$. Then R is an integral domain, as it is a sub-ring of $\mathbb{Q}[t]$. And the units units of R are $R^* = \{-1, 1\}$ only, as $fg = 1$ implies both $f(0)g(0) = 1$ and $\deg(f) = 0 = \deg(g)$. However R neither is noetherian, nor an UFD, as it contains the following infinitely ascending chain of principal ideals

$$tR \subset \frac{1}{2}tR \subset \ldots \subset \frac{1}{2^n}tR \subset \frac{1}{2^{n+1}}tR \subset \ldots$$

[the inclusion is strict, as 2 is not a unit of R]. (Also the ideal $t\mathbb{Q}[t] \trianglelefteq_{\mathrm{i}} R$ is not finitely generated, as else there would be some $a \in \mathbb{Z}$ such that $at\mathbb{Q}[t] \subseteq t\mathbb{Z}[t]$, which is absurd). Yet it can be proved that R is a Bezout domain (see [Dummit, Foote, 9.3, exercise 5] for hints on this).

(ii) We want to present another example of a Bezout domain: Fix any field $(E, +, \cdot)$ and let S be the polynomial ring in countably many variables $S := E[t_k \mid k \in \mathbb{N}]$. Let us denote the ideal

$$\mathfrak{u} := \langle t_k - t_{k+1}^2 \mid k \in \mathbb{N} \rangle_{\mathrm{i}} \trianglelefteq_{\mathrm{i}} S$$

Then $R := S/\mathfrak{u}$ is a Bezout domain (refer to [Dummit, Foote, 9.2, exercise 12] for hints). However it is no noetherian ring (in particular no PID), as the following ideal $\mathfrak{a}$ of R is *not* finitely generated

$$\mathfrak{a} := \langle t_k + \mathfrak{u} \mid k \in \mathbb{N} \rangle_{\mathrm{i}} \trianglelefteq_{\mathrm{i}} R$$

(iii) ($\diamondsuit$) Let us denote denote the integral closure of $\mathbb{Z}$ in $\mathbb{C}$ by $\mathcal{O}$: To stay self-contained: Let us denote $\mathbb{Z}[t]_1 := \{t^n + a_1 t^{n-1} + \cdots + a_n \in \mathbb{Z}[t] \mid n \in \mathbb{N},\ a_i \in \mathbb{Z}\}$) the set of monic polynomials over $\mathbb{Z}$, then $\mathcal{O}$ is the set of $z \in \mathbb{C}$ that satisfy an equation of the form $f(z) = 0$ for some $f \in \mathbb{Z}[t]_1$

$$\mathcal{O} := \{z \in \mathbb{C} \mid \exists f \in \mathbb{Z}[t]_1 : f(z) = 0\}$$

E.g. $\sqrt{2} \in \mathcal{O}$, as $\sqrt{2}$ satisfies the equation $t^2 - 1$, but $1/2 \notin \mathcal{O}$, as this would require $2t - 1$ to be a factor of the equation. The integral closure always is a sub-ring (and in particular an integral domain, as $\mathbb{C}$ is a field). In fact $\mathcal{O}$ is a Bezout domain that satisfies $\mathrm{Spec}(\mathcal{O}) = \mathrm{Smax}(\mathcal{O}) \cup \{0\}$ (see [Dummit, Foote, chapter 16.3, exercise 23] for hints on how to prove this). However $\mathcal{O}$ neither is noetherian, nor an UFD, as it contains the following infinitely ascending chain of principal ideals

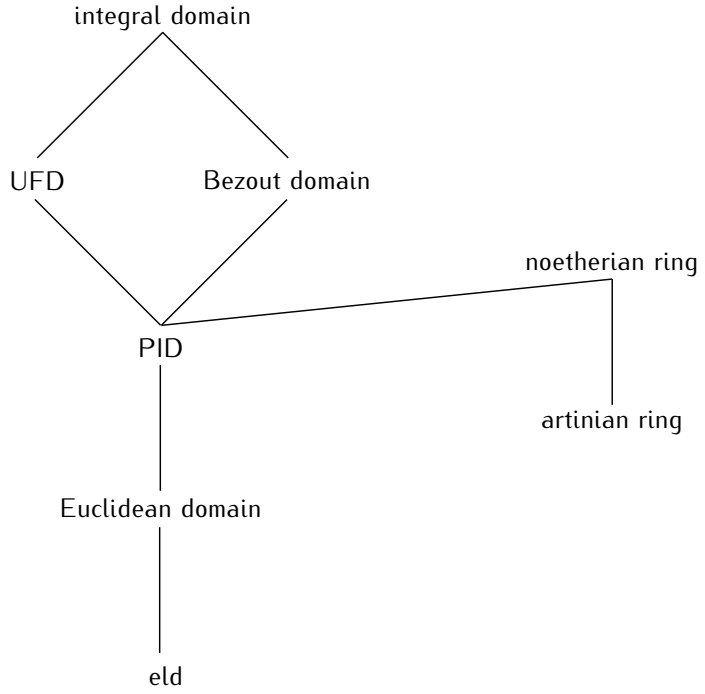
$$2\mathcal{O} \subset \sqrt{2}\mathcal{O} \subset \sqrt[4]{2}\mathcal{O} \subset \ldots \subset \sqrt[2^n]{2}\mathcal{O} \subset \sqrt[2^{n+1}]{2}\mathcal{O} \subset \ldots$$

(iv) Consider $\omega := (1 + i\sqrt{19})/2 \in \mathbb{C}$ and consider the following sub-ring $\mathbb{Z}[\omega] := \{a + b\omega \mid a, b \in \mathbb{Z}\}$ of $\mathbb{C}$. Then we obtain a Dedekind-Hasse norm on $\mathbb{Z}[\omega]$ by letting

$$\delta : \mathbb{Z}[\omega] \to \mathbb{N} : a + b\omega \mapsto a^2 + ab + 5b^2$$

(this is proved in [Dummit, Foote, page 282]). In particular $\mathbb{Z}[\omega]$ is a PID by virtue of (2.82.(ii)). However $\mathbb{Z}[\omega]$ is *not* an Euclidean domain (under any function ν whatsoever). The latter statement is proved in [Dummit, Foote, page 277].

(2.87) Remark:
By now we have studied a quite respectable list of different kinds of commutative rings from integral domains and fields over noetherian rings to Bezout domains. Thereby we have found several inclusions, that we wish to summarize in the diagram below:



Note however that every single inclusion in this diagram is strict. E.g. there are integral domains that are not Bezout domains and there are PIDs that are not Euclidean domains. The following table presents examples of rings R that satisfy one property, but not the next stronger one

R	is	is not
$\mathbb{Z}[\sqrt{-3}]$	noetherian integral domain	UFD
$\mathbb{Z}+t\mathbb{Q}[t]$	Bezout domain	noetherian, UFD
$\mathbb{Q}[s,t]$	noetherian UFD	Bezout domain
$\mathbb{Z}[(1+\sqrt{-19})/2]$	PID	Euclidean domain
$\mathbb{Z}$	Euclidean domain	field, artinian ring

2.8 Lasker-Noether Decomposition

Primary decomposition is a very strong property and as such something that is not satisfied often. Historically ideals have been introduced by Richard Dedekind to be ideal numbers, that are better behaved, than the elements of the algebraic number fields themselves. For example take a look at the following ring

$$\mathbb{Z}[\sqrt{-5}] \;:=\; \mathbb{Z}[t] \Big/ (t^2+5)\mathbb{Z}[t]$$

The element $x := t + (t^2+5)\mathbb{Z}[t]$ satisfies $x^2 + 5 = 0$ and is hence denoted as $\sqrt{-5} := x$. An isomorphic realization of this ring is the sub-ring of $\mathbb{C}$ generated by the single element $x := 5i \in \mathbb{C}$. This element can be used to present two primary decompositions of 6 that are *not* essentially equal:

$$6 \;=\; 2 \cdot 3 \;=\; \left(1-\sqrt{-5}\right)\left(1+\sqrt{-5}\right)$$

Remember that according to (2.59) in a noetherian integral domain we always have a decomposition of an element into irreducible elements - problem is that this decomposition is far from unique. That is the reason why we had to regard prime elements instead. In this section we will try to remedy this by decomposing whole ideals instead of elements of a noetherian ring.

It turns out that this decomposition of ideals is closely related to decomposing geometric objects (varieties) into smaller parts. That also is the application where the notions of *isolated* and *embedded* components come from (which will be introduced, later on). But this has to be left for a course in algebraic geometry.

Note that the noetherian and factorial properties are completely independent of one and another: E.g. $\mathbb{Z}[\sqrt{-5}]$ is noetherian, but not factorial, whereas $\mathbb{Z}[t_i \mid i \in \mathbb{N}]$ is factorial, but not noetherian. But we will see, that in case of noetherian UFDs both theories coincide.

In order to begin by defining the basic notion of a primary ideal, we will use the set $\mathrm{ZD}(R)$ of *zero-divisors* and the *nil-radical* $\mathrm{NIL}(R)$ of a ring R and the set $\mathrm{ZD}_R(M)$ of *zero-divisors* of an R-module M. This has not been introduced yet, but we will only use it in the case $M = R/\mathfrak{a}$. Also we give a survey of these notions in the remark following the definition.

In the definition to come, we will see, that a primary ideal is similar to a prime ideal, but somewhat weaker: If a product ab is contained in the primary ideal $\mathfrak{a}$ then only one of them needs to be contained in $\mathfrak{a}$, the other may belong to the radical $\sqrt{\mathfrak{a}}$ only:

(2.88) Definition: (viz. 1058)
Let $(R, +, \cdot)$ be a commutative ring and $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be a proper (i.e. $\mathfrak{a} \neq R$) ideal of R. Then $\mathfrak{a}$ is said to be a **primary** ideal of R, iff it satisfies one of the following equivalent conditions

(a) The radical of $\mathfrak{a}$ contains the set of zero-divisors of $R/\mathfrak{a}$ (as an R-module)

$$\mathrm{ZD}_R\left(R \Big/ \mathfrak{a}\right) \;\subseteq\; \sqrt{\mathfrak{a}}$$

(b) In the ring $R/\mathfrak{a}$ the set of zero-divisors is contained in the nil radical

$$\mathrm{ZD}\left(R \Big/ \mathfrak{a}\right) \;\subseteq\; \mathrm{NIL}\left(R \Big/ \mathfrak{a}\right)$$

(c) The set of zero-divisors of $R/\mathfrak{a}$ (as a ring) equals the nil-radical of $R/\mathfrak{a}$

$$\text{ZD}\left(R\Big/\mathfrak{a}\right) \;=\; \text{NIL}\left(R\Big/\mathfrak{a}\right)$$

(d) For any two elements $a, b \in R$ of R we obtain the following implication

$$ab \in \mathfrak{a},\ b \notin \mathfrak{a} \quad\Longrightarrow\quad a \in \sqrt{\mathfrak{a}}$$

(e) For any two elements $a, b \in R$ of R we obtain the following implication

$$ab \in \mathfrak{a},\ b \notin \sqrt{\mathfrak{a}} \quad\Longrightarrow\quad a \in \mathfrak{a}$$

And if $\mathfrak{a}$ is a primary ideal, then it is customary to say that $\mathfrak{a}$ is **associated** to (the prime ideal) $\sqrt{\mathfrak{a}}$. Finally the set of all primary ideals of R is said to be the **primary spectrum** of R and we will abbreviate this by $\text{Spri}(R)$. And if $\mathfrak{p} \in \text{Spec}(R)$ is a prime ideal of R, then we denote the set of all primary ideals of R associated to $\mathfrak{p}$, by $\text{Spri}_{\mathfrak{p}}(R)$

$$\begin{aligned}\text{Spri}(R) &:= \{\,\mathfrak{a} \trianglelefteq_{\text{i}} R \mid \mathfrak{a} \neq R,\ (\text{a})\,\}\\ \text{Spri}_{\mathfrak{p}}(R) &:= \left\{\,\mathfrak{a} \in \text{Spri}(R) \;\middle|\; \sqrt{\mathfrak{a}} = \mathfrak{p}\,\right\}\end{aligned}$$

Nota clearly associateness is an equivalence relation on $\text{Spri}(R)$. That is for any primary ideals $\mathfrak{a}$ and $\mathfrak{b} \trianglelefteq_{\text{i}} R$ we let $\mathfrak{a} \approx \mathfrak{b} :\Longleftrightarrow \sqrt{\mathfrak{a}} = \sqrt{\mathfrak{b}}$ and thereby $\approx$ is an equivalence relation on $\text{Spri}(R)$. Further if $\mathfrak{p} = \sqrt{\mathfrak{a}}$, then $\text{Spri}_{\mathfrak{p}}(R)$ is precisely the equivalence class of $\mathfrak{a}$ under $\approx$.

(2.89) Remark:
In the definition above there already appeared the notion of zero-divisors of a module (which will be introduced in 3.2). Thus we wish to shortly present what this means in the context here. Let $(R, +, \cdot)$ be a commutative ring and $\mathfrak{a} \trianglelefteq_{\text{i}} R$ be an ideal [and M be an R-module]. Then the set of *zero-divisors* of $M = R/\mathfrak{a}$ as an R-module will be defined to be

$$\begin{aligned}\text{ZD}_R(M) &= \{\,a \in R \mid x \in M\ :\ x \neq 0 \text{ and } ax = 0\,\}\\ \text{ZD}_R\left(R\Big/\mathfrak{a}\right) &= \left\{\,a \in R \;\middle|\; \exists\, b+\mathfrak{a} \in R\Big/\mathfrak{a}\ :\ b+\mathfrak{a} \neq 0+\mathfrak{a} \text{ and } a(b+\mathfrak{a}) = 0\,\right\}\\ &= \left\{\,a \in R \;\middle|\; \exists\, b+\mathfrak{a} \in R\Big/\mathfrak{a}\ :\ b \notin \mathfrak{a} \text{ and } ab \in \mathfrak{a}\,\right\}\end{aligned}$$

as $b + \mathfrak{a} = 0 + \mathfrak{a}$ is equivalent to $b \in \mathfrak{a}$ [by construction of $R/\mathfrak{a}$] and because of the identity $a(b+\mathfrak{a}) = ab + \mathfrak{a} = (a+\mathfrak{a})(b+\mathfrak{a})$ [which is just the definition of the scalar multiplication of $R/\mathfrak{a}$ as an R-module, resp. of the multiplication in the ring $R/\mathfrak{a}$]. Now take a look at the set of zero-divisors of $R/\mathfrak{a}$ as a ring

$$\begin{aligned}\text{ZD}\left(R\Big/\mathfrak{a}\right) &= \left\{\,a+\mathfrak{a} \in R\Big/\mathfrak{a} \;\middle|\; \exists\, b+\mathfrak{a} \in R\Big/\mathfrak{a}\ :\ b+\mathfrak{a} \neq 0+\mathfrak{a} \text{ and } (a+\mathfrak{a})(b+\mathfrak{a}) = 0\,\right\}\\ &= \left\{\,a+\mathfrak{a} \in R\Big/\mathfrak{a} \;\middle|\; \exists\, b+\mathfrak{a} \in R\Big/\mathfrak{a}\ :\ b \notin \mathfrak{a} \text{ and } ab \in \mathfrak{a}\,\right\}\end{aligned}$$

We find that the condition $b \notin \mathfrak{a}$ and $ab \in \mathfrak{a}$ in both of these sets coincides. From this we find, that $a \in \mathrm{zd}_R(R/\mathfrak{a})$ is equivalent to $a + \mathfrak{a} \in \mathrm{zd}(R/\mathfrak{a})$. In a more compact notation, this can be put as

$$\mathrm{zd}\left(R\Big/\mathfrak{a}\right) \;=\; \mathrm{zd}_R(R/\mathfrak{a})\Big/\mathfrak{a}$$

(2.90) Proposition: (viz. 1059)
Let $(R,+,\cdot)$ be a commutative ring and $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be an ideal. Then we the following statements are true

(i) Any prime ideal of R already is primary. That is we obtain the following inclusion of the spectra

$$\mathrm{Spec}(R) \;\subseteq\; \mathrm{Spri}(R)$$

(ii) If $\mathfrak{a}$ is a primary ideal of R, then the radical $\sqrt{\mathfrak{a}}$ is a prime ideal of R. In fact it is the uniquely determined, smallest prime ideal containing $\mathfrak{a}$, that is we obtain the following implications

$$\mathfrak{a} \in \mathrm{Spri}(R) \;\Longrightarrow\; \sqrt{\mathfrak{a}} \in \mathrm{Spec}(R)$$

$$\mathfrak{a} \in \mathrm{Spri}(R) \;\Longrightarrow\; \left\{\sqrt{\mathfrak{a}}\right\} = \{\,\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{a} \subseteq \mathfrak{p}\,\}_*$$

(iii) If $\mathfrak{m} := \sqrt{\mathfrak{a}}$ is a maximal ideal of R, then $\mathfrak{a}$ is a primary ideal of R associated to $\mathfrak{m}$. Put formally

$$\sqrt{\mathfrak{a}} \in \mathrm{Smax}(R) \;\Longrightarrow\; \mathfrak{a} \in \mathrm{Spri}(R)$$

(iv) Suppose that $\mathfrak{m} \in \mathrm{Smax}(R)$ is a maximal ideal of R, such that there is some $k \in \mathbb{N}$ such that $\mathfrak{m}^k \subseteq \mathfrak{a} \subseteq \mathfrak{m}$. Then $\mathfrak{a}$ is a primary ideal of R associated to $\mathfrak{m}$. That is we obtain the implication

$$\mathfrak{m}^k \subseteq \mathfrak{a} \subseteq \mathfrak{m} \;\Longrightarrow\; \mathfrak{a} \in \mathrm{Spri}_{\mathfrak{m}}(R)$$

(v) If $\mathfrak{a}_1, \ldots, \mathfrak{a}_k \trianglelefteq_{\mathrm{i}} R$ are finitely many primary ideals of R, all associated to the same pirme ideal $\mathfrak{p} = \sqrt{\mathfrak{a}_i}$. Then their intersection is a primary ideal associated to $\mathfrak{p}$, too

$$\{\,\mathfrak{a}_1, \ldots, \mathfrak{a}_k\,\} \subseteq \mathrm{Spri}_{\mathfrak{p}}(R) \;\Longrightarrow\; \bigcap_{i=1}^{k} \mathfrak{a}_i \in \mathrm{Spri}_{\mathfrak{p}}(R)$$

(vi) If $u \in R$ and $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ is a primary ideal, with $\mathfrak{p} := \sqrt{\mathfrak{a}}$, then we get the following statements concerning the ideal $\mathfrak{a} : u = \{\, a \in R \mid au \in \mathfrak{a}\,\}$

(1) if $u \in \mathfrak{a}$ then $\mathfrak{a} : u = R$

(2) if $u \notin \mathfrak{a}$ then $\mathfrak{a} : u \in \mathrm{Spri}_{\mathfrak{p}}(R)$

(3) if $u \notin \mathfrak{p}$ then $\mathfrak{a} : u = \mathfrak{a}$

(vii) Consider a homomorphism $\varphi : R \to S$ between the commutative rings $(R,+,\cdot)$ and $(S,+,\cdot)$. If now $\mathfrak{b} \trianglelefteq_{\mathrm{i}} S$ is a primary ideal of S, then $\mathfrak{a} := \varphi^{-1}(\mathfrak{b})$ is a primary ideal of R. And if $\mathfrak{q} := \sqrt{\mathfrak{b}}$ denotes the ideal $\mathfrak{b}$ is associated to, then $\mathfrak{a}$ is associated to $\varphi^{-1}(\mathfrak{q})$. Formally that is

$$\mathfrak{b} \in \mathrm{Spri}_{\mathfrak{q}}(S) \;\Longrightarrow\; \varphi^{-1}(\mathfrak{b}) \in \mathrm{Spri}_{\varphi^{-1}(\mathfrak{q})}(R)$$

(viii) ($\diamondsuit$) Let $U \subseteq R$ be a multiplicatively closed set, $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ be a prime ideal of R with $\mathfrak{p} \cap U = \emptyset$ and denote by $\mathfrak{q} := U^{-1}\mathfrak{p} \trianglelefteq_{\mathrm{i}} U^{-1}R$ the corresponding prme ideal of $U^{-1}R$. Then we obtain a one-to-one correspondence, by

$$\begin{array}{rcl} \mathrm{Spri}_{\mathfrak{p}}(R) & \longleftrightarrow & \mathrm{Spri}_{\mathfrak{q}}(U^{-1}R) \\ \mathfrak{a} & \mapsto & U^{-1}\mathfrak{a} \\ \mathfrak{b} \cap R & \hookleftarrow & \mathfrak{b} \end{array}$$

(2.91) Example: (viz. 1060)

(i) Let $(R, +, \cdot)$ be an integral domain and $p \in R$ be a prime element of R. Then for any $1 \leq n \in \mathbb{N}$ the ideal $\mathfrak{a} := p^n R$ is primary and associated, to the prime ideal $\sqrt{\mathfrak{a}} = pR$.

(ii) In a PID $(R, +, \cdot)$ the primary ideals are precisely the ideals 0 and $p^n R$ for some $p \in R$ prime. Formally that is the identity

$$\mathrm{Spri}(R) \;=\; \{\, p^n R \mid 1 \leq n \in \mathbb{N},\ p \in R \text{ prime} \,\} \cup \{0\}$$

(iii) Primary ideals do *not* need to be powers of prime ideals. As an example let $(E, +, \cdot)$ be any field and consider $R := E[s,t]$. Then the ideal $\mathfrak{a} := \langle s, t^2 \rangle_{\mathrm{i}}$ is primary and associated to the maximal ideal $\mathfrak{m} := \langle s, t \rangle_{\mathrm{i}}$. In fact we get $\mathfrak{m}^2 \subset \mathfrak{a} \subset \mathfrak{m}$ and hence there is *no* prime ideal $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ such that $\mathfrak{a} = \mathfrak{p}^k$ for some $k \in \mathbb{N}$.

(iv) Powers of prime ideals do *not* need to be primary ideals. As an example let $(E, +, \cdot)$ be any field again and consider $R := E[s,t,u]/\mathfrak{u}$ where $\mathfrak{u} := \langle u^2 - st \rangle_{\mathrm{i}}$. Let us denote $a := s + \mathfrak{u}$, $b := t + \mathfrak{u}$ and $c := u + \mathfrak{u}$. Then we obtain a prime ideal $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ by letting $\mathfrak{p} := \langle b, c \rangle_{\mathrm{i}}$. However we will see that $\mathfrak{a} := \mathfrak{p}^2$ is no primary ideal.

(2.92) Proposition: (viz. 1061)
Let $(R, +, \cdot)$ be a commutative ring and $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be a proper ideal of R, i.e. $\mathfrak{a} \neq R$. For any $n \in \mathbb{N}$ we define the n-th *symbolic power* $\mathfrak{a}^{(n)}$ of $\mathfrak{a}$ to be the following subset of R:

$$\mathfrak{a}^{(n)} \;:=\; \{\, a \in R \mid \exists\, u \in R \setminus \mathfrak{a} : au \in \mathfrak{a}^n \,\}$$

If $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ is a prime ideal of R and $n \geq 1$, then the n-th symbolic power of $\mathfrak{p}$ is an ideal of R, that contains $\mathfrak{p}^n$ and that satisfies some further properties, namely

(i) $\mathfrak{p}^n \subseteq \mathfrak{p}^{(n)} \subseteq \mathfrak{p}$

(ii) $\forall\, n \in \mathbb{N}$ we get $\mathfrak{p}^{(n+1)} \subseteq \mathfrak{p}^{(n)}$

(iii) $\mathfrak{p}^{(n)}$ is a primary ideal, with $\sqrt{\mathfrak{p}^{(n)}} = \mathfrak{p}$

(iv) Recall the notion of the ideal $\mathfrak{a}R_{\mathfrak{p}} = \{\, a/u \in R_{\mathfrak{p}} \mid a \in \mathfrak{a}, u \in R \setminus \mathfrak{p} \,\}$ in the localisation $R_{\mathfrak{p}}$, then

$$\mathfrak{p}^{(n)} R_{\mathfrak{p}} \;=\; \mathfrak{p}^n R_{\mathfrak{p}}$$

(2.93) Definition:
Let $(R,+,\cdot)$ be a commutative ring, then a proper ideal $\mathfrak{p}$ is said to be **irreducible** iff it is not the intersection of finitely many larger ideals. That is iff $\mathfrak{p}$ satisfies the following three properties

(1) $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ is an ideal

(2) $\mathfrak{p} \neq R$ is proper

(3) for any $\mathfrak{a}, \mathfrak{b} \trianglelefteq_{\mathrm{i}} R$ we have $\mathfrak{p} = \mathfrak{a} \cap \mathfrak{b} \implies \mathfrak{p} = \mathfrak{a}$ or $\mathfrak{p} = \mathfrak{b}$

(2.94) Theorem: (viz. 1062)

(i) Let $(R,+,\cdot)$ be a commutative ring, then any prime ideal of R already is irreducible. That is for any ideal $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ we get the implication

$$\mathfrak{p} \text{ prime} \implies \mathfrak{p} \text{ irreducible}$$

(ii) Let $(R,+,\cdot)$ be a noetherian ring, then any irreducible ideal of R already is primary. That is for any ideal $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ we get the implication

$$\mathfrak{p} \text{ irreducible} \implies \mathfrak{p} \text{ primary}$$

(iii) Let $(R,+,\cdot)$ be a noetherian ring, then any proper ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$, $\mathfrak{a} \neq R$ admits an irreducible decomposition $(\mathfrak{p}_1,\ldots,\mathfrak{p}_k)$: There are ideals $\mathfrak{p}_i \trianglelefteq_{\mathrm{i}} R$ (where $i \in 1\ldots k$ and $1 \leq k \in \mathbb{N}$) such that

(1) $\forall\, i \in 1\ldots k \,:\, \mathfrak{p}_i$ is an irreducible ideal

(2) $\mathfrak{a} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_k$

(2.95) Definition:
Let $(R,+,\cdot)$ be a commutative ring and $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be an ideal of R. Then a tupel $\mathcal{A} = (\mathfrak{a}_1,\ldots,\mathfrak{a}_k)$ is said to be a **primary decomposition** of $\mathfrak{a}$, iff it satisfies both of the properties

(1) $\forall\, i \in 1\ldots k \,:\, \mathfrak{a}_i \in \mathrm{Spri}(R)$ is a primary ideal of R

(2) $\mathfrak{a} = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_k$

And $(\mathfrak{a}_1,\ldots,\mathfrak{a}_k)$ is said to be **minimal** (or **irredundant**) iff we further get the following two properties

(3) $\forall\, j \in 1\ldots k \,:\, \mathfrak{a} \neq \bigcap_{i\neq j} \mathfrak{a}_i$

(4) $\forall\, i \neq j \in 1\ldots k \,:\, \sqrt{\mathfrak{a}_i} \neq \sqrt{\mathfrak{a}_j}$

Finally if $\mathcal{A} = (\mathfrak{a}_1,\ldots,\mathfrak{a}_k)$ is a minimal primary decomposition of $\mathfrak{a}$, then let us denote $\mathfrak{p}_i := \sqrt{\mathfrak{a}_i}$. These ideals are called the *associated prime ideals* of $\mathfrak{a}$. Those $\mathfrak{a}_i$ that belong to minimal $\mathfrak{p}_i$ are known as *isolated components*. Those $\mathfrak{a}_i$ that are not isolated components, are said to be *embedded components*:

$$\begin{aligned} \mathrm{ass}(\mathcal{A}) &:= \{\, \mathfrak{p}_1,\ldots,\mathfrak{p}_k \,\} \\ \mathrm{iso}(\mathcal{A}) &:= \{\, \mathfrak{a}_i \mid i \in 1\ldots k,\ \mathfrak{p}_i \in \mathrm{ass}(\mathcal{A})_* \,\} \end{aligned}$$

$$\begin{aligned} &= \left\{ \mathfrak{a}_i \;\middle|\; i \in 1\ldots k,\ \forall j \in 1\ldots k : \mathfrak{p}_j \subseteq \mathfrak{p}_i \implies j = i \right\} \\ \operatorname{emb}(\mathcal{A}) &:= \{\, \mathfrak{a}_1, \ldots, \mathfrak{a}_k \,\} \setminus \operatorname{iso}(\mathcal{A}) \end{aligned}$$

(2.96) Example:
Let $(R, +, \cdot)$ be an UFD and $a \in R$ with $0 \neq a \notin R^*$. Then we pick up a primary decomposition of a, that is $a = p_1^{n_1} \ldots p_k^{n_k}$ where $1 \leq k \in \mathbb{N}$ and for any $i, j \in 1\ldots k$ we have $p_i \in R$ is prime, $1 \leq n_i \in \mathbb{N}$ and $p_i R = p_j R$ implies $i = j$. Then we obtain a minimal primary decomposition of $\mathfrak{a} = aR$

$$(\mathfrak{a}_1, \ldots, \mathfrak{a}_k) \quad \text{where} \quad \mathfrak{a}_i := p_i^{n_i} R$$

And for this primary decomposition we find $\mathfrak{p}_i := \sqrt{\mathfrak{a}_i} = p_i R$ and hence no embedded components, but

$$\begin{aligned} \operatorname{ass}(\mathfrak{a}_1, \ldots, \mathfrak{a}_k) &= \{\, \mathfrak{p}_1, \ldots, \mathfrak{p}_k \,\} \\ \operatorname{iso}(\mathfrak{a}_1, \ldots, \mathfrak{a}_k) &= \{\, \mathfrak{a}_1, \ldots, \mathfrak{a}_k \,\} \end{aligned}$$

(2.97) Remark:
So why would we call an intersection $\mathfrak{a} = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_k$ a *decomposition* of $\mathfrak{a}$? As in fact we think of a decomposition of $R/\mathfrak{a}$. Clearly, if $\mathfrak{a} = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_k$ then we find an injective homomorphism of rings

$$R \Big/ \mathfrak{a} \hookrightarrow \bigoplus_{i=1}^{k} R \Big/ \mathfrak{a}_i \ : \ b + \mathfrak{a} \mapsto (b + \mathfrak{a}_1, \ldots, b + \mathfrak{a}_k)$$

Prob the well-definedness is due to $\mathfrak{a} \subseteq \mathfrak{a}_i$ and (1.75) and the homomorphism properties are clear. And if $(b + \mathfrak{a}_i) = (c + \mathfrak{a}_i)$ then $b - c \in \mathfrak{a}_i$ for any $i \in 1\ldots k$ such that $b - c \in \mathfrak{a}$, which is $b + \mathfrak{a} = c + \mathfrak{a}$, whence we get the injectivity.
And if any $\mathfrak{a}_i$ is primary, then $\operatorname{zd}(R/\mathfrak{a}_i) = \operatorname{nil}(R/\mathfrak{a}_i)$ so $R/\mathfrak{a}$ is contained in a somewhat special ring. In this sense we will generalize this to the primary decomposition of modules, in section 5.1.

(2.98) Proposition: (viz. 1063)
Let $(R, +, \cdot)$ be a commutative ring and $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be an ideal of R. If $\mathfrak{a}$ admits any primary decomposition, then it already admits a minimal primary decomposition. To be precise: Let $(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$ be any primary decomposition of $\mathfrak{a}$ then we obtain a minimal primary decomposition of $\mathfrak{a}$ by

(1) For any (non-empty) subset $N \subseteq 1\ldots n$ let us denote the intersection of all the $\mathfrak{a}_i$ for $i \in N$ by

$$\mathfrak{a}_N := \bigcap_{i \in N} \mathfrak{a}_i$$

Then we choose some $M \subseteq 1\ldots n$ with a minimal number of elements, such that $\mathfrak{a}_M = \mathfrak{a}$. That is $\mathfrak{a}_M = \mathfrak{a}$ but for any $L \subset M$ we have $\mathfrak{a}_L \neq \mathfrak{a}$.

(2) Now intersect all $\mathfrak{a}_i$ (where $i \in M$) that belong to the same prime ideal. That is we define an equivalence relation on M letting $i \approx j \ :\Longleftrightarrow\ \sqrt{\mathfrak{a}_i} = \sqrt{\mathfrak{a}_j}$. If we take to the quotient set $A := M/\approx$, then we have found a minimal primary decomposition $(\mathfrak{a}_\alpha)$ of $\mathfrak{a}$ (where $\alpha \in A$).

(2.99) Proposition: (viz. 1063)
Let $(R,+,\cdot)$ be a commutative ring, $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be a proper $\mathfrak{a} \neq R$ ideal and consider $(\mathfrak{a}_1,\ldots,\mathfrak{a}_k)$ a minimal primary decomposition of $\mathfrak{a}$. Let us further denote $\mathfrak{p}_i := \sqrt{\mathfrak{a}_i}$, then we obtain the following statements

(i) Clearly all the primary ideals and all the associated primary ideals of the decomposition are pairwise distinct, that is we have

$$\#\{\,\mathfrak{a}_1,\ldots,\mathfrak{a}_k\,\} \;=\; \#\{\,\mathfrak{p}_1,\ldots,\mathfrak{p}_k\,\} \;=\; k$$

(ii) For any $u \in R$ we obtain the following identity (where by convention the intersection over the empty set is defined to be the ring R itself)

$$\sqrt{\mathfrak{a} : u} \;=\; \bigcap \{\,\mathfrak{p}_i \mid i \in 1\ldots k,\; u \notin \mathfrak{a}_i\,\}$$

(iii) The prime ideals associated to $\mathfrak{a}$ are independent of the specific primary decomposition $(\mathfrak{a}_1,\ldots,\mathfrak{a}_k)$ chosen, as they can be described, as

$$\mathrm{ass}(\mathfrak{a}_1,\ldots,\mathfrak{a}_k) \;=\; \mathrm{Spec}(R) \cap \left\{\, \sqrt{\mathfrak{a} : u} \;\middle|\; u \in R \,\right\}$$

(iv) $(\diamondsuit)$ If $\mathfrak{p}_i$ is minimal among $\mathrm{ass}(\mathfrak{a}_1,\ldots,\mathfrak{a}_k)$ then we can reconstruct $\mathfrak{a}_i$ from $\mathfrak{a}$ and $\mathfrak{p}_i$. To be precise for any $i \in 1\ldots k$ we get

$$\mathfrak{p}_i \in \mathrm{ass}(\mathfrak{a}_1,\ldots,\mathfrak{a}_k)_* \quad\Longrightarrow\quad \mathfrak{a} : (R \setminus \mathfrak{p}_i) = \mathfrak{a}_i$$

(v) $(\diamondsuit)$ The isolated components of $\mathfrak{a}$ are independent of the specific primary decomposition $(\mathfrak{a}_1,\ldots,\mathfrak{a}_k)$ chosen, as they can be described, as

$$\mathrm{iso}(\mathfrak{a}_1,\ldots,\mathfrak{a}_k) \;=\; \{\,\mathfrak{a} : (R \setminus \mathfrak{p}) \;\mid\; \mathfrak{p} \in \mathrm{ass}(\mathfrak{a}_1,\ldots,\mathfrak{a}_k)_*\,\}$$

(2.100) Remark: $(\diamondsuit)$
In the items (iii) and (v) of the proposition we have seen, that the sets of associated prime ideals resp. of isolated components of an ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ are given to be the following:

$$\begin{aligned}
\mathrm{ass}(\mathfrak{a}) &:= \mathrm{Spec}(R) \cap \left\{\, \sqrt{\mathfrak{a} : u} \;\middle|\; u \in R \,\right\} \\
\mathrm{iso}(\mathfrak{a}) &:= \{\,\mathfrak{a} : (R \setminus \mathfrak{p}) \;\mid\; \mathfrak{p} \in \mathrm{ass}(\mathfrak{a})_*\,\}
\end{aligned}$$

That is if $(\mathfrak{a}_1,\ldots,\mathfrak{a}_k)$ is *any* minimal primary decomposition of $\mathfrak{a}$, then $\mathrm{ass}(\mathfrak{a}_1,\ldots,\mathfrak{a}_k) = \mathrm{ass}(\mathfrak{a})$ and $\mathrm{iso}(\mathfrak{a}_1,\ldots,\mathfrak{a}_k) = \mathrm{iso}(\mathfrak{a})$. In section 5.1 we will introduce the notion of a prime ideal *associated* to an R-module M. Thus if $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ is an ideal, then it makes sense to the regard the prime ideals associated to $\mathfrak{a}$ as an R-module. And by definition this is just

$$\begin{aligned}
\mathrm{Sann}(\mathfrak{a}) &= \mathrm{Spec}(R) \cap \{\,\mathrm{ann}(a) \mid a \in \mathfrak{a}\,\} \\
&= \mathrm{Spec}(R) \cap \{\,0 : a \mid a \in \mathfrak{a}\,\}
\end{aligned}$$

(where the equality is due to $\mathrm{ann}(a) = 0 : a$ for any $a \in R$). Thus we find that at a first glance $\mathrm{Sann}(\mathfrak{a})$ has *absolutely nothing* to do with $\mathrm{ass}(\mathfrak{a})$. However it will turn out that the set $\mathrm{ass}(\mathfrak{a})$ is closely related to the set of associated prime ideals of the R-module $R/\mathfrak{a}$. By definition that is

$$\begin{aligned}\mathrm{Sann}_R\left(R\Big/\mathfrak{a}\right) &:= \mathrm{Spec}(R) \cap \left\{ \mathrm{ann}_R(x) \;\middle|\; x \in R\Big/\mathfrak{a} \right\} \\ &= \mathrm{Spec}(R) \cap \{\, \mathrm{ann}_R(b+\mathfrak{a}) \mid b \in R \,\} \\ &= \mathrm{Spec}(R) \cap \{\, \mathfrak{a} : b \mid b \in R \,\}\end{aligned}$$

(the latter equality is due to $\mathrm{ann}_R(b+\mathfrak{a}) = \mathfrak{a} : b$ for any $b \in R$ again). Thus the difference between this set and $\mathrm{ass}(\mathfrak{a})$ lies in the fact that $\mathrm{ass}(\mathfrak{a})$ allows the taking of radicals. Hence it is easy to see that $\mathrm{Sann}_R(R/\mathfrak{a}) \subseteq \mathrm{ass}(\mathfrak{a})$. In section 5.1 we will prove that for noetherian rings R we even have

$$\mathrm{Sann}_R\left(R\Big/\mathfrak{a}\right) = \mathrm{ass}(\mathfrak{a})$$

(2.101) Corollary: (viz. 1065) **Lasker-Noether**
Let $(R,+,\cdot)$ be a noetherian ring, then any proper ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$, $\mathfrak{a} \neq R$ admits a minimal primary decomposition. And in this decomposition the associated prime ideals and the isolated components are uniquely determined by $\mathfrak{a}$. Formally that is

(1) There are ideals $\mathfrak{a}_i \trianglelefteq_{\mathrm{i}} R$ (where $i \in 1 \ldots k$ and $1 \leq k \in \mathbb{N}$) such that $(\mathfrak{a}_1, \ldots, \mathfrak{a}_k)$ is a minimal primary decomposition of $\mathfrak{a}$.

(2) If $(\mathfrak{a}_1, \ldots, \mathfrak{a}_k)$ and $(\mathfrak{b}_1, \ldots, \mathfrak{b}_l)$ are any two minimal primary decompositions of $\mathfrak{a}$ then we obtain the following three identities

$$\begin{aligned} k &= l \\ \mathrm{ass}(\mathfrak{a}_1, \ldots, \mathfrak{a}_k) &= \mathrm{ass}(\mathfrak{b}_1, \ldots, \mathfrak{b}_l) \\ \mathrm{iso}(\mathfrak{a}_1, \ldots, \mathfrak{a}_k) &= \mathrm{iso}(\mathfrak{b}_1, \ldots, \mathfrak{b}_l) \end{aligned}$$

(3) If $\mathfrak{a} = \sqrt{\mathfrak{a}}$ is a radical ideal, then the minimal primary decomposition $(\mathfrak{a}_1, \ldots, \mathfrak{a}_k)$ of $\mathfrak{a}$ is uniquely determined (up to ordering) and consists precisely of the prime ideals minimal over $\mathfrak{a}$, formally

$$\{\, \mathfrak{a}_1, \ldots, \mathfrak{a}_k \,\} = \{\, \mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{a} \subseteq \mathfrak{p} \,\}_*$$

(2.102) Corollary: (viz. 1066)
Let $(R,+,\cdot)$ be a noetherian ring and $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be a proper ideal of R (that is $\mathfrak{a} \neq R$). If now $\mathfrak{q} \trianglelefteq_{\mathrm{i}} R$ is any prime ideal of R then we obtain

(i) $\mathfrak{a}$ is contained in $\mathfrak{q}$ iff $\mathfrak{q}$ contains an associated prime ideal of $\mathfrak{a}$ iff $\mathfrak{q}$ contains an isolated component of $\mathfrak{a}$. Formally that is

$$\begin{aligned} \mathfrak{a} \subseteq \mathfrak{q} &\iff \exists\, \mathfrak{p} \in \mathrm{ass}(\mathfrak{a}) \,:\, \mathfrak{p} \subseteq \mathfrak{q} \\ &\iff \exists\, \mathfrak{i} \in \mathrm{iso}(\mathfrak{a}) \,:\, \mathfrak{i} \subseteq \mathfrak{q} \end{aligned}$$

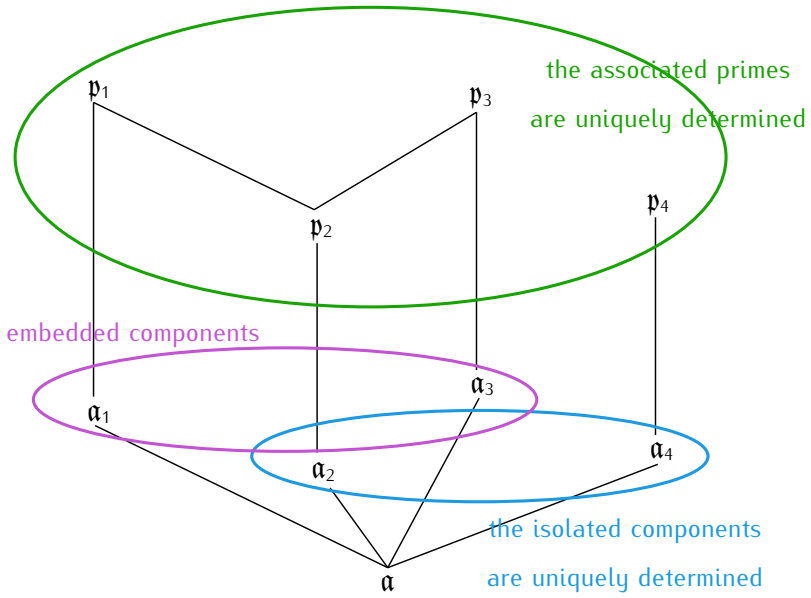
(ii) The set of primes lying minimally over $\mathfrak{a}$ is precisely the set of primes belonging to the isolated components of $\mathfrak{a}$. Formally again

$$\{\, \mathfrak{q} \in \operatorname{Spec}(R) \mid \mathfrak{a} \subseteq \mathfrak{q} \,\}_* \;=\; \operatorname{ass}(\mathfrak{a})_*$$

(iii) And thereby the radical of $\mathfrak{a}$ is precisely the intersection of all (minimal) associated prime ideals of $\mathfrak{a}$. Put formally that is

$$\sqrt{\mathfrak{a}} \;=\; \bigcap \operatorname{ass}(\mathfrak{a}) \;=\; \bigcap \operatorname{ass}(\mathfrak{a})_*$$

(2.103) Remark:
The following diagram should help to illustrate the situation a little: Suppose $(R, +, \cdot)$ is a noetherian ring and $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ is a proper $\mathfrak{a} \neq R$ ideal of R and pick up a minimal primary decomposition on $\mathfrak{a}$. As an example consider a decomposition of the following form: In this diagram



there are 4 associated primes $\mathfrak{p}_1$ to $\mathfrak{p}_4$. However both $\mathfrak{p}_1$ and $\mathfrak{p}_3$ contain $\mathfrak{p}_2$. Conversely $\mathfrak{p}_2$ and $\mathfrak{p}_4$ are the minimal associated primes of $\mathfrak{a}$. Hence $\mathfrak{q}_2$ and $\mathfrak{q}_4$ are the isolated components of $\mathfrak{a}$, whereas $\mathfrak{q}_1$ and $\mathfrak{q}_3$ are embedded components of $\mathfrak{a}$. From this we know that $\mathfrak{q}_2$ and $\mathfrak{q}_4$ are part of any minimal primary decomposition of $\mathfrak{a}$, whereas $\mathfrak{q}_1$ and $\mathfrak{q}_3$ may vary. Also the associated primes $\mathfrak{p}_1$ to $\mathfrak{p}_4$ always are uniquely determined. Thereby $\mathfrak{p}_2$ and $\mathfrak{p}_4$ are the prime ideals of R lying minimally over $\mathfrak{a}$ and hence

$$\sqrt{\mathfrak{a}} \;=\; \mathfrak{p}_2 \cap \mathfrak{p}_4$$

(2.104) Example:
Fix any field $(F,+,\cdot)$ and let $R := F[s,t]$ be the polynomial ring over E in s and t (note that R is noetherian due to Hilbert's basis theorem). Now consider the ideal $\mathfrak{a} := \langle s^2, st\rangle_{\mathfrak{i}}$. Then we obtain two distinct primary decompositions $(\mathfrak{a}_1,\mathfrak{a}_2)$ and $(\mathfrak{b}_1,\mathfrak{b}_2)$ of $\mathfrak{a}$ by letting

$$\begin{array}{lccc} & \mathfrak{a}_i & \mathfrak{b}_i & \mathfrak{p}_i \\ i=1 & \langle s\rangle_{\mathfrak{i}} & \langle s\rangle_{\mathfrak{i}} & \langle s\rangle_{\mathfrak{i}} \\ i=2 & \langle s^2,st,t^2\rangle_{\mathfrak{i}} & \langle s^2,t\rangle_{\mathfrak{i}} & \langle s,t\rangle_{\mathfrak{i}} \end{array}$$

where $\mathfrak{p}_i := \sqrt{\mathfrak{a}_i} = \sqrt{\mathfrak{b}_i}$. It is no coincidence that both primary decompositions have 2 elements and that the radicals $\mathfrak{p}_i$ are equal. Further $\mathfrak{p}_1 \subset \mathfrak{p}_2$, that is $\mathfrak{a}_1 = \mathfrak{b}_1$ are isolated components of $\mathfrak{a}$ and $\mathfrak{a}_2 \neq \mathfrak{b}_2$ are embedded components (of the decompositions). In fact this example demonstrates that the embedded components may be different.

$$\begin{aligned} \operatorname{ass}(\mathfrak{a}) &= \{\, sR, sR+tR \,\} \\ \operatorname{iso}(\mathfrak{a}) &= \{\, sR \,\} \end{aligned}$$

2.9 Finite Rings

(2.105) Definition: (viz. 1066)
Let $(R,+,\cdot)$ be any ring, denote its zero element by 0_R and its unit element by 1_R. For any $1 \leq k \in \mathbb{N}$ let us denote $k_R := k1_R = 1_R + \cdots + 1_R$ (k-times). Then there exists a uniquely determined homomrphism of rings ζ from $\mathbb{Z}$ to R, and this is given to be

$$\zeta \ : \ \mathbb{Z} \to R \ : \ k \mapsto \begin{cases} k_R \text{ if } k > 0 \\ 0_R \text{ if } k = 0 \\ -(-k)_R \text{ if } k < 0 \end{cases}$$

The image of ζ in R is said to be the **prime ring** of R and denoted by $\text{PRR}(R)$. In fact it is the smallest sub-ring of R in the following sense: it is the intersection of *all* sub-rings of R. Formally

$$\text{PRR}(R) \ := \ \text{im}(\zeta) \ = \ \bigcap \{ P \mid P \ \leq_{\text{r}} \ R \}$$

And the kernel of ζ is an ideal in $\mathbb{Z}$. Hence (as $\mathbb{Z}$ is a PID) there is a uniquely determined $n \in \mathbb{N}$ such that $\text{kn}(\zeta) = n\mathbb{Z}$. This number n is said to be the **characteristic** of R, denoted by

$$\text{CHAR}(R) \ := \ n \quad \text{where} \quad \text{kn}(\zeta) \ = \ n\mathbb{Z}$$

That is if R has characteristic zero $n = 0$, then we get $k_R = 0 \implies k = 0$. And if R has non-zero characteristic $n \neq 0$, then n is precisely the smallest number such that $n_R = 0$. Formally that is

$$\text{CHAR}(R) \ = \ \min\{ 1 \leq k \in \mathbb{N} \mid k_R = 0 \}$$

Also by construction of ζ and the first isomorphism theorem, if $n = \text{CHAR}(R)$ is the characteristic of R and we denote $\mathbb{Z}_0 := \mathbb{Z}$ and $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ for $n \geq 1$, then $\mathbb{Z}_n$ is embedded into R under

$$\mathbb{Z}_n \ \hookrightarrow \ R \ : \ k + n\mathbb{Z} \ \mapsto \ k_R$$

(2.106) Remark:
If $(F,+,\cdot)$ even is a field, we may also introduce the **prime field** of F (denoted by $\text{PRF}(F)$) to be the intersection of all subfields of F. Formally

$$\text{PRF}(F) \ := \ \bigcap \{ E \mid E \ \leq_{\text{f}} \ F \}$$

And if is easy to see that $\text{PRF}(F)$ is precisely the quotient field of the prime ring $\text{PRR}(F)$. Formally that is the following identity

$$\text{PRF}(F) \ = \ \left\{ ab^{-1} \mid a,b \in \text{PRR}(F),\ b \neq 0 \right\}$$

Prob as $E \ \leq_{\text{f}} \ F$ implies $E \ \leq_{\text{r}} \ F$ (by definition) we have $\text{PRR}(F) \subseteq \text{PRF}(F)$. Let us now denote the quotient field of $\text{PRR}(F)$ by $Q \subseteq F$. As $\text{PRF}(F)$ is a field and $\text{PRR}(F) \subseteq \text{PRF}(F)$ it is clear that $Q \subseteq \text{PRF}(F)$. On the other hand $Q \leq_{\text{f}} F$ is a subfield and hence we have $\text{PRF}(F) \subseteq Q$ by construction. Together this means $\text{PRF}(F) = Q$ as claimed.

(2.107) Proposition: (viz. 1067)
Let $(R,+,\cdot)$ be any ring, then the characteristic of R satisfies the following properties

(i) If $R \neq 0$ is a non-zero integral domain, then the characteristic of R is a prime number or zero. Formally that is the following implication

$$R \text{ integral domain, } R \neq 0 \quad \Longrightarrow \quad \text{CHAR}(R) = 0 \text{ or prime}$$

(ii) R has characteristic zero if and only if the prime ring of R is isomorphic to $\mathbb{Z}$. More precisely we find the following equivalences

$$\begin{aligned} \text{CHAR}(R) = 0 \quad &\Longleftrightarrow \quad \forall\, k \in \mathbb{N} \,:\, k_R = 0 \implies k = 0 \\ &\Longleftrightarrow \quad \mathbb{Z} \;\cong_{\mathrm{r}}\; \text{PRR}(R) : k \mapsto \zeta(k) \end{aligned}$$

(iii) R has non-zero characteristic $n = \text{CHAR}(R) > 0$ if and only if the prime ring of R is isomorphic to $\mathbb{Z}_n$. More precisely for any $1 \leq n \in \mathbb{N}$ we find the equivalence of the following statements

$$\begin{aligned} \text{CHAR}(R) = n \quad &\Longleftrightarrow \quad n = \min\{\, 1 \leq k \in \mathbb{N} \mid k_R = 0 \,\} \\ &\Longleftrightarrow \quad \mathbb{Z}_n \;\cong_{\mathrm{r}}\; \text{PRR}(R) : k + n\mathbb{Z} \mapsto \zeta(k) \end{aligned}$$

(iv) Now suppose that R is a field, then the prime field of R is given to be

$$\begin{aligned} \text{CHAR}(R) = 0 \quad &\Longleftrightarrow \quad \mathbb{Q} \;\cong_{\mathrm{r}}\; \text{PRF}(R) \\ \text{CHAR}(R) = p \neq 0 \quad &\Longleftrightarrow \quad \mathbb{Z}_p \;\cong_{\mathrm{r}}\; \text{PRF}(R) \end{aligned}$$

(v) Let $(R,+,\cdot)$ be a finite ring (that is $\#R < \infty$), then the characteristic of R is non-zero and divides the number of elements of R, formally once more

$$0 \neq \;\; \text{CHAR}(R) \mid \#R$$

(2.108) Example: (viz. 1068)
Fix $n \in \mathbb{N}$ and recall $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. In case $n = 0$ we have $n\mathbb{Z} = 0$ and hence $\mathbb{Z}_n = \mathbb{Z}$, which is an integral domain. In case $n = 1$ we have $n\mathbb{Z} = \mathbb{Z}$ and hence $\mathbb{Z}_n = 0$ is the zero-ring. And in case $n \geq 2$ we get the following equivalencies

(a) n is a prime number

(b) $\mathbb{Z}_n$ is a (finite) field

(c) $\mathbb{Z}_n$ is an integral domain

We even get a concrete description of the unit group of $\mathbb{Z}_n$: For any $n \geq 2$ the set of units of $\mathbb{Z}_n$ is given to be the set of all $k + n\mathbb{Z}$ such that k is relatively prime to n. Formally that is

$$\mathbb{Z}_n^* \;\; = \;\; \{\, k + n\mathbb{Z} \mid 1 \in \gcd(k,n) \,\}$$

Nota It is worthwhile to note that this matches (2.107.(i)) and (2.109.(i)). We also find a generalisation of this in (2.112) to the case of non-commutative rings. So while we could use all these propositions and theorems to patch together an abstract proof, we decided to give direct, autonomous argument.

(2.109) Proposition: (viz. 1069)

(i) Let $(R,+,\cdot)$ be a finite (that is $\#R < \infty$), commutative ring. Then the non-zero divisors of R already are invertible, such that we get the equality

$$R^* \;=\; R \setminus \mathrm{zd}(R)$$

(ii) Let $(F,+,\cdot)$ be any field and $G \leq_{\mathrm{g}} F^*$ be a subgroup of the multiplicative group of F. If G is finite then it already is cyclic (that is there is some $g \in G$ such that $G = \{1, g, g^2, \ldots, g^{n-1}\}$, where $n = \#G$ is the order of G). In particular the multiplicative group $(F^*,\cdot)$ of any finite field F is cyclic.

$$\#G < \infty \text{ finite} \quad \Longrightarrow \quad G \text{ cyclic}$$

(iii) Let $(F,+,\cdot)$ be a finite field $n := \#F$ the number of elements of F. Then for any $a \in F$ we have $a^n = a$ and we even find the following identity of polynomials in $F[t]$

$$\prod_{a \in F} (t - a) \;=\; t^n - t$$

(iv) Let $(S,+,\cdot)$ be an integral domain and consider a prime element $p \in S$. Let further $1 \leq n \in \mathbb{N}$ and denote the quotient ring $R := S/p^nS$. Then the set of zero-divisors of R is precisely the ideal generated by the residue class of p. Formally that is

$$\mathrm{zd}(R) \;=\; (p + p^nS)\,R$$

(v) Now let $(S,+,\cdot)$ be a PID, consider a prime element $p \in S$ and let $R := S/p^nS$ again. Then we obtain the following statements

$$\mathrm{nil}(R) \;=\; \mathrm{zd}(R) \;=\; R \setminus R^* \;=\; (p + p^nS)\,R$$

$$\mathrm{Spec}(R) \;=\; \mathrm{Smax}(R) \;=\; \{\, \mathrm{nil}(R) \,\}$$

(vi) Let $(R,+,\cdot)$ be any noetherian (in particular commutative) ring and fix any $1 \leq m \in \mathbb{N}$. Then there only are finitely many prime ideals $\mathfrak{p}$ of R such that $R/\mathfrak{p}$ has at most m elements. Formally

$$\#\left\{ \mathfrak{p} \in \mathrm{Spec}(R) \;\middle|\; \#{}^{R}\!\big/_{\mathfrak{p}} \leq m \right\} \;<\; \infty$$

(2.110) Remark: $(\diamondsuit)$
As in (iv) let $(S,+,\cdot)$ be a PID, $p \in S$ be a prime element and define $R := S/p^nS$ again. Then we have seen, that $\text{NIL}(R) = R \setminus R^*$ and we will later call a ring with such a property a local ring. To be precise: R is a *local ring* with maximal ideal $\text{NIL}(R)$. Further - in a fancier language - the property $\text{Spec}(R) = \text{Smax}(R)$ can be reformulated as "R is a *zero-dimensional* ring".

(2.111) Example:
The field of complex numbers $\mathbb{C}$ has an infinite subgroup of its multiplicative group $\mathbb{C}^*$, namely the one-dimensional torus $\mathbb{T} = \{ z \in \mathbb{C} \mid |z| = 1 \} = \{ a + ib \in \mathbb{C} \mid a^2 + b^2 = 1 \}$. We also get finite subgroups of $\mathbb{C}$ by fixing $1 \leq n \in \mathbb{N}$ and taking to

$$g_n \;:=\; \exp\left(\frac{2\pi}{n} i\right)$$

Then $\mathbb{T}_n := \{ g_n^k \mid k \in \mathbb{Z} \} = \{ 1, g, g^2, \ldots, g^{n-1} \}$ is a subgroup of $\mathbb{T}$, which is a subgroup of $\mathbb{C}^*$ in turn. In fact these are the only finite subgroups of $\mathbb{C}^*$, as the subgroups generator has to have absoulte value 1 (as it's n-th power is 1 and the absolute value is multiplicative).

(2.112) Theorem: (viz. 1072) **of Wedderburn**
Let $(F,+,\cdot)$ be an arbitrary ring with finitely many elements only (formally $\#F < \infty$), then the following three statements are equivalent

(a) F is a field

(b) F is a skew-field

(c) F is an integral domain

Fragments - algebra - rings: Frobenius automorphsim - proposition 11 to corollary 16

2.10 Localization of Rings

Localization is one of the most powerful and fundamental tools in commutative algebra - and luckily one of the most simple ones. The general idea of localization is to start with a commutative ring $(R,+,\cdot)$, to designate a sufficient subset $U \subseteq R$ and to enlarge R to the ring $U^{-1}R$ in which the elements of $u \in U \subseteq R \subseteq U^{-1}R$ now are units. And it will turn out, that in doing this the ideal structure of $U^{-1}R$ will be *easier* than that of R. And conversely we can restore information of R by regarding sufficiently many localizations of R (this will be the *local-global-principle*). These two properties give the method of localizing its punch. In fact commutative algebra has been most successful with problems that allowed localization. So let us finally begin with the fundamental definitions:

(2.113) Definition:
Let $(R,+,\cdot)$ be any commutative ring, then a subset $U \subseteq R$ is said to be **multiplicatively closed** iff it satisfies the following two properties

$$\begin{aligned} 1 &\in U \\ u,v \in U &\implies uv \in U \end{aligned}$$

And $U \subseteq R$ is said to be a **saturated** mutilplicative system, iff conversely the factors u and v of a product uv belonging to U already had to be elements of U. That is iff U satisfies

$$\begin{aligned} 1 &\in U \\ u,v \in U &\implies uv \in U \\ uv \in U &\implies u \in U \end{aligned}$$

(2.114) Proposition: (viz. 1074)

(i) In a commutative ring $(R,+,\cdot)$ the set R^* of units and the set $\mathrm{NZD}(R)$ of non-zero-divisors of R both are saturated multiplicatively closed subsets of R.

(ii) If $U \subseteq R$ is a saturated, multiplicatively closed set, then $R^* \subseteq U$, as for any $u \in R^*$ we get $uu^{-1} = 1 \in U$ and hence $u \in U$.

(iii) If U, $V \subseteq R$ are any multiplicatively closed sets in the commutative ring R, then their product $UV := \{\, uv \mid u \in U, v \in V \,\}$ is multiplicatively closed, too.

(iv) If $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ is an ideal, then $1 + \mathfrak{a} \subseteq R$ is a multiplicatively closed subset.

(v) Let $\varphi : R \to S$ be a ring-homomorphism between the commutative rings R and S and consider $U \subseteq R$ and $V \subseteq V$. Then we get

$$\begin{array}{lcll} U & \text{mult. closed} & \implies & \varphi(U) \quad \text{mult. closed} \\ V & \text{mult. closed} & \implies & \varphi^{-1}(V) \quad \text{mult. closed} \\ V & \text{saturated} & \implies & \varphi^{-1}(V) \quad \text{saturated} \end{array}$$

(vi) If $\mathcal{U} \subseteq \mathcal{P}(R)$ is a chain (under $\subseteq$) of multiplicatively closed subsets of R, then the union $\bigcup \mathcal{U} \subseteq R$ is a multiplicatively closed set again.

(vii) If $\mathcal{U} \subseteq \mathcal{P}(R)$ is a non-empty ($\mathcal{U} \neq \emptyset$) family of [saturated] multiplicatively closed subsets of R, then the intersection $\bigcap \mathcal{U} \subseteq R$ is a [saturated] multiplicatively closed set, too.

NOTA this allows to define the *multiplicative closure* of a subset A of R to be the smallest multiplicatively closed set containing A, which is $\bigcap \{ U \subseteq R \mid A \subseteq U, U \text{ multiplicatively closed} \}$. Likewise we may define the *saturated multiplicative closure* of A to be the intersection of all saturated multiplicatively closed subsets containing A.

(viii) As an example consider any $u \in R$, then the set $U := \{ u^k \mid k \in \mathbb{N} \}$ clearly is a multiplicatively closed set. In fact it is the smallest multiplicatively closed set containing u. That is U is the multiplicative closure of $\{ u \}$.

(ix) Let $U \subseteq R$ be a multiplicatively closed subset of R, then the saturated multiplicative closure $\overline{U}$ of U can be given explicitly to be the set

$$\overline{U} \;=\; \{ a \in R \mid \exists\, b \in R, \exists\, u, v \in U : uab = uv \}$$

(2.115) Proposition: (viz. 1075)
Let $(R, +, \cdot)$ be any commutative ring and $U \subseteq R$ be a subset. Then U is saturated multiplicatively closed, iff it is the complement of a union of prime ideals of R. Formally that is the equivalence of

(a) $\exists\, \mathcal{P} \subseteq \operatorname{Spec}(R)$ such that $U = R \setminus \bigcup \mathcal{P}$

(b) $U \subseteq R$ is a saturated multiplicatively closed subset

(2.116) Definition: (viz. 1075)
Let $(R, +, \cdot)$ be any commutative ring and $U \subseteq R$ be a multiplicatively closed subset of R. Then we obtain an equivalence relation $\sim$ on the set $U \times R$ by virtue of (with $a, b \in R$ and $u, v \in U$)

$$(u, a) \sim (v, b) \quad :\Longleftrightarrow \quad \exists\, w \in U \;:\; vwa = uwb$$

And we denote the quotient of $U \times R$ modulo $\sim$ by $U^{-1}R$ and the equivalence class of (u, a) is denoted by a/u, formally this is the following construction

$$\begin{aligned} \frac{a}{u} &:= \{ (v, b) \in U \times R \mid (u, a) \sim (v, b) \} \\ U^{-1}R &:= U \times R \Big/ \sim \end{aligned}$$

Now $U^{-1}R$ becomes a commutative ring under the following addition and multiplication of its elements

$$\begin{aligned} \frac{a}{u} + \frac{b}{v} &:= \frac{av + bu}{uv} \\ \frac{a}{u} \cdot \frac{b}{v} &:= \frac{ab}{uv} \end{aligned}$$

It is clear that under these operations the zero-element of $U^{-1}R$ is given to be $0/1$ and the unit element of $U^{-1}R$ is given to be $1/1$. And we obtain a canonical ring homomorphism from R to $U^{-1}R$ by letting

$$\kappa \;:\; R \to U^{-1}R \;:\; a \mapsto \frac{a}{1}$$

In general this canonical homomorphism need not be and embedding (i.e. injective). Yet we do obtain the following equivalences regarding this homomorphism

$$\begin{aligned} \kappa \text{ injective} &\iff U \subseteq \text{NZD}(R) \\ \kappa \text{ bijective} &\iff U \subseteq R^* \end{aligned}$$

(2.117) Remark:

- Though the equivalence relation $\sim$ in the above definition might look a little artificial at first sight nothing here is mythical or mere chance. To see this let us first consider the case of an integral domain $(R, +, \cdot)$. Then we may divide by w and hence we get

 $$\frac{a}{u} = \frac{b}{v} \iff va = ub$$

 and this is just what we expect, if we multiply the left-hand equation by uv. To allow a common factor w is just the right way to deal with zero divisors in R. For convenience we repeat the defining property of the quotient a/u for general commutative rings $(R, +, \cdot)$

 $$\frac{a}{u} = \frac{b}{v} \iff \exists\, w \in U \;:\; vwa = uwb$$

- And from this equivalence it is immediately clear that fractions a/u in $U^{-1}R$ can be reduced by common factors v of U. That is for any elements $a \in R$ and $u, v \in U$ we have the equality

 $$\frac{av}{uv} = \frac{a}{u}$$

 And this allows to express sums by going to a common denominator. That is consider $a_1, \ldots, a_n \in R$ and $u_1, \ldots, u_n \in U$. Then we denote $u := u_1 \ldots u_n \in U$ and $\widehat{u}_i := u/u_i \in U$ (e.g. $\widehat{u}_1 = u_2 \ldots u_n$). Then we have just remarked that $a_i/u_i = (a_i\widehat{u}_i)/u$ and thereby

 $$\frac{a_1}{u_1} + \cdots + \frac{a_n}{u_n} = \frac{a_1\widehat{u}_1 + \cdots + a_n\widehat{u}_n}{u}$$

- This equivalence also yields that $1/1 = 0/1$ holds true in $U^{-1}R$ if and only if the multiplicatively closed set contains zero $0 \in U$. But as $0/1$ is the zero-element and $1/1$ is the unit element of $U^{-1}R$ we thereby found another equivalence

 $$U^{-1}R = 0 \iff 0 \in U$$

- As we have intended, localizing turns the elements $u \in U$ into units of $U^{-1}R$. More precisely if $U \subseteq R$ is multiplicatively closed, then we obtain

$$\left(U^{-1}R\right)^* \quad \supseteq \quad \left\{ \frac{au}{v} \;\middle|\; a \in R^*, u, v \in U \right\}$$

 Prob consider any au/v such that $a \in R^*$ and u, $v \in U$, then we compute $(au/v)(a^{-1}v/u) = (aa^{-1}uv)/(uv) = (uv)/(uv) = 1/1$ and hence au/v is a unit, with inverse $(au/v)^{-1} = a^{-1}v/u$.

 Nota However the equality need not hold true! As an example consider the integers $R = \mathbb{Z}$ and let $U = \left\{ 6^k \mid k \in \mathbb{N} \right\} = \{1, 6, 36, \dots\}$. Then $2/1$ is invertible, with inverse $(2/1)^{-1} = 3/6$, yet $2/1$ is not of the form $R^*U/U = \left\{ \pm 6^k \mid k \in \mathbb{Z} \right\} \subseteq \mathbb{Q}$.

- If $U \subseteq R$ even is a saturated multiplicatively closed subset, then we obtain a complete description of the units of $U^{-1}R$ to be the fractions u/v of elements u, $v \in U$. Formally that is

$$\left(U^{-1}R\right)^* \quad = \quad \left\{ \frac{u}{v} \;\middle|\; u, v \in U \right\}$$

 Prob clearly u/v is a unit of $U^{-1}R$, since $(u/v)^{-1} = v/u$. Conversely if b/v is a unit of $U^{-1}R$ there is some $a/u \in U^{-1}R$ such that $ab/uv = (a/u)(b/v) = 1/1$. That is there is some $w \in U$ such that $abw = uvw$. Hence $b(aw) = uvw \in U$ and as U is saturated this implies $b \in U$.

- Let $(R, +, \cdot)$ be a commutative ring and $U \subseteq R$ be a multiplicatively closed set, such that $U^{-1}R$ is finitely generated as an R-module. That is there are $b_1, \dots, b_n \in R$ and $v_1, \dots . v_n \in U$ such that

$$U^{-1}R \quad = \quad \left\{ \frac{a_1 b_1}{v_1} + \cdots + \frac{a_n b_n}{v_n} \;\middle|\; a_1, \dots, a_n \in R \right\}$$

 Then the canonical mapping $\kappa : R \to U^{-1}R : b \mapsto b/1$ is surjective. Prob consider any $a/u \in U^{-1}R$ and denote $v := v_1 \dots v_n \in U$ and $\widehat{v}_i := v/v_i \in V$ (e.g. $\widehat{v}_1 = v_2 \dots v_n$). As $uv \in V$ and $U^{-1}R$ is generated by the b_i/v_1 there are $a_1, \dots, a_n \in R$ such that

$$\frac{a}{uv} \quad = \quad \frac{a_1 b_1}{v_1} + \cdots + \frac{a_n b_n}{v_n} \quad = \quad \frac{a_1 b_1 \widehat{v}_1 + \cdots + a_n b_n \widehat{v}_n}{v}$$

 That is there is some $w \in U$ such that $vwa = uvwb$ where we let $b := a_1 b_1 \widehat{v}_1 + \cdots + a_n b_n \widehat{v}_n \in R$. That is we have found $(vw)1a = (vw)ub$, thus by definition we have $\kappa(b) = b/1 = a/u$. And as a/u has been arbitrary this is the surjectivity of κ.

- If $U \subseteq R$ is multiplicatively closed and we consider $R \subseteq R[t]$ as a subset of the polynomial ring $R[t]$, then we will see in (2.132.(i)) that the localisation of the polynomial ring is just the same as the polynomial ring of the localisation. That is we have the following isomorphism of rings

$$\begin{array}{rcl} U^{-1}\big(R[t]\big) & \cong_{\mathrm{r}} & \big(U^{-1}R\big)[t] \\ \dfrac{f}{u} & \mapsto & \displaystyle\sum_{k=0}^{\infty} \frac{f[k]}{u} t^k \end{array}$$

(2.118) Example:
Let now $(R,+,\cdot)$ be any commutative ring. Then we present three examples that are of utmost importance. Hence the reader is asked to regard these examples as definitions of the objects R_u, $\mathrm{QUOT}(R)$ and $R_\mathfrak{p}$.

- If R is an integral domain and $0 \notin U$, then $a/u = b/v$ is equivalent, to $va = ub$, as we can eliminate $w \neq 0$ from $w(va - ub) = 0$. In particular for $U = R \setminus \{0\}$ the construction of $U^{-1}R$ can be simplified somewhat: First let $Q := \{\, (a,u) \in R^2 \mid u \neq 0 \,\}$, then we obtain an equivalence relation on Q by letting $(a,u) \sim (b,v) \;:\Longleftrightarrow\; va = ub$. Let us denote the equivalence class of (a,u) by $a/u := [(a,u)]$ again. Then we have regained the **quotient field** of R as in section 1.4

$$\mathrm{QUOT}(R) \;=\; \left\{ \frac{a}{b} \;\middle|\; a,b \in R,\ b \neq 0 \right\}$$

 Note that this is precisely the construction that is used to obtain $\mathbb{Q}$ from $\mathbb{Z}$. If now $U \subseteq R$ is an arbitrary multiplicatively closed set satisfying $0 \notin U$, then the localization of R in U is canonically isomorphic to the following sub-ring of the quotient field:

$$U^{-1}R \;\cong_\mathrm{r}\; \left\{ \frac{a}{u} \in \mathrm{QUOT}(R) \;\middle|\; a \in R, u \in U \right\} \;:\; \frac{a}{u} \mapsto \frac{a}{u}$$

 Prob we will first prove the well-definedness and injectivity: By definition $a/u = b/v$ in $U^{-1}R$ is equivalent to $w(av - bu) = 0$ for some $w \in U$. But as $0 \notin U$ we get $w \neq 0$ and hence $av = bu$, as R is an integral domain. This again is just $a/u = b/v$ in $\mathrm{QUOT}(R)$. The surjectivity of the map is obvious and it clearly is a homomorphism, as the algebraic operations are literally the same.

- Let us generalize the previous construction a little: It is clear that the set $U := \mathrm{NZD}(R)$ of non-zero divisors of R is a saturated multiplicatively closed set. Thus we may define the **total ring of fractions** of a commutative ring R to be the localization in this set

$$\mathrm{QUOT}(R) \;:=\; (\mathrm{NZD}R)^{-1} R$$

 Note that in case of an integral domain we have $\mathrm{NZD}(R) = R \setminus \{0\}$ and hence we obtain precisely the same ring as before. Further note that by the very nature of $U = \mathrm{NZD}(R)$ the canonical homomorphism κ is injective. That is we can always regard R as a sub-ring of $\mathrm{QUOT}(R)$

$$R \hookrightarrow \mathrm{QUOT}(R) \;:\; a \mapsto a/1 \text{ is injective}$$

 And as $\mathrm{NZD}(R)$ is saturated we can give the units of $\mathrm{QUOT}(R)$ explicitly

$$(\mathrm{QUOT}(R))^* \;=\; \left\{ \frac{u}{v} \;\middle|\; u,v \in \mathrm{NZD}(R) \right\}$$

 In particular we find that $\mathrm{QUOT}(R)$ is a field if and only if $\mathrm{NZD}(R) = R \setminus \{0\}$ and this is precisely the property of R being an integral domain. That is we obtain the equivalence

$$R \text{ integral domain} \;\Longleftrightarrow\; \mathrm{QUOT}(R) \text{ field}$$

- Consider some field $(F,+,\cdot)$ and a sub-ring $R \leq_{\mathrm{r}} F$. In particular $R \neq 0$ is a non-zero integral domain and hence $\mathrm{QUOT}(R)$ is a field. Let us now denote the subfield of F generated by R by E, which is given to be

$$E \;:=\; \left\{ ab^{-1} \mid a,b \in R \right\}$$

Then is is straightforward to check that the algebraic operations on the quotient field $\mathrm{QUOT}(R)$ coincide with those of the field E. That is we obtain a well-defined isomorphism of rings

$$\mathrm{QUOT}(R) \;\cong_{\mathrm{r}}\; E \;:\; \frac{a}{b} \mapsto ab^{-1}$$

- Consider any $u \in R$, then clearly $U := \left\{ 1, u, u^2, u^3, \ldots \right\}$ is multiplicatively closed. Hence we obtain a commutative ring by localizing

$$R_u \;:=\; \left\{ u^k \;\middle|\; k \in \mathbb{N} \right\}^{-1} R$$

in which $u = u/1$ is invertible (with inverse $1/u$). By the remarks above it is clear that $R_u = 0$ is zero if and only if u is a nilpotent of R. And $R \hookrightarrow R_u$ is embedded under κ if and only if u is a non-zero divisor of R, respectively isomorphic if u is a unit. Altogether

$$\begin{aligned} R_u = 0 \quad &\Longleftrightarrow \quad u \in \mathrm{NIL}(R) \\ \kappa : R \hookrightarrow R_u \quad &\Longleftrightarrow \quad u \in \mathrm{NZD}(R) \\ \kappa : R \cong_{\mathrm{r}} R_u \quad &\Longleftrightarrow \quad u \in R^* \end{aligned}$$

- In (2.12) and (in a more general version) in (2.115) we have seen, that the complement $R \setminus \mathfrak{p}$ of a prime ideal $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ is a saturated, multiplicatively closed set. Thus for prime ideals $\mathfrak{p}$ we may always define the localization

$$R_{\mathfrak{p}} \;:=\; (R \setminus \mathfrak{p})^{-1} R$$

And by going to complements it is clear that R is embedded into $R_{\mathfrak{p}}$ under κ, iff $\mathfrak{p}$ is contained in the set of zero divisors of R

$$\kappa : R \hookrightarrow R_{\mathfrak{p}} \quad \Longleftrightarrow \quad \mathfrak{p} \subseteq \mathrm{ZD}(R)$$

In any case - as $R \setminus \mathfrak{p}$ is saturated multiplicatively closed subset - we can explicitly describe the group of units of $R_{\mathfrak{p}}$ to be

$$(R_{\mathfrak{p}})^* \;=\; \left\{ \frac{u}{v} \;\middle|\; u,v \notin \mathfrak{p} \right\}$$

- If $(R,+,\cdot)$ is an integral domain and $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ is a prime ideal of R then we get an easy alternative description of the localized ring $R_{\mathfrak{p}}$: Let $E := \mathrm{QUOT}(R)$ be the quotient field of R, then we denote:

$$E_{\mathfrak{p}} \;:=\; \left\{ \frac{a}{b} \in E \;\middle|\; b \notin \mathfrak{p} \right\}$$

And thereby we obtain a canonical isomorphism from the localized ring $R_{\mathfrak{p}}$ to $E_{\mathfrak{p}}$ by $a/b \mapsto a/b$

$$R_{\mathfrak{p}} \;\cong_{\mathrm{r}}\; E_{\mathfrak{p}} \;:\; \frac{a}{b} \mapsto \frac{a}{b}$$

One might be tempted to say $R_\mathfrak{p} = E_\mathfrak{p}$, but - from a set-theoretical point of view - this is not quite true, as the equivalence class $a/b \in R_\mathfrak{p}$ only is a subset of $a/b \in E_\mathfrak{p}$. Note that under this isomorphism the maximal ideal $\mathfrak{m}_\mathfrak{p} := \mathfrak{p}R_\mathfrak{p} = (R \setminus \mathfrak{p})^{-1}\mathfrak{p}$ (that is induced by $\mathfrak{p}$) in $R_\mathfrak{p}$ corresponds to the following maximal ideal in $E_\mathfrak{p}$

$$\mathfrak{m}_\mathfrak{p} \quad \longleftrightarrow \quad \left\{ \frac{a}{b} \in E \;\middle|\; a \in \mathfrak{p},\ b \notin \mathfrak{p} \right\}$$

(2.119) Proposition: (viz. 1084)
Consider any two commutative rings $(R, +, \cdot)$ and $(S, +, \cdot)$, a multiplicatively closed set $U \subseteq R$ and a homomorphism $\varphi : R \to S$ of rings. Then $\varphi(U) \subseteq S$ is mutiplicatively closed again and we obtain a well-defined homomorphism of rings of the form

$$U^{-1}\varphi \;:\; U^{-1}R \to \varphi(U)^{-1}S \;:\; \frac{a}{u} \mapsto \frac{\varphi(a)}{\varphi(u)}$$

Thereby if φ is injective, surjective or bijective, then $U^{-1}\varphi$ satisfies the same property.

(2.120) Proposition: (viz. 1085)
Universal Property: Let $(R, +, \cdot)$ and $(S, +, \cdot)$ be commutative rings, $U \subseteq R$ be a multiplicatively closed subset and $\varphi : R \to S$ be a homomorphism of rings, such that $\varphi(U) \subseteq S^*$. Then there is a uniquely determined homomorphism of rings $\overline{\varphi} : U^{-1}R \to S$ such that $\overline{\varphi}\kappa = \varphi$. And this is given to be

$$\overline{\varphi} \;:\; U^{-1}R \to S \;:\; \frac{a}{u} \mapsto \varphi(a)\,\varphi(u)^{-1}$$

(2.121) Remark:
Let $(R, +, \cdot)$ be a commutative ring and $U, V \subseteq R$ be multiplicatively closed sets, such that $U \subseteq V$. Further consider the canonical homomorphism $\kappa : R \to V^{-1}R : a \mapsto a/1$. Then it is clear that $\kappa(U) \subseteq (V^{-1}R)^*$, as the inverse of $u/1$ is given to be $1/u$. Thus by the above proposition we obtain an induced homomorphism of the form

$$\overline{\kappa} \;:\; U^{-1}R \to V^{-1}R \;:\; \frac{a}{u} \mapsto \frac{a}{u}$$

Thereby $\overline{\kappa}(a/u) = 0/1$ iff there is some $v \in V$ such that $va = 0$. And this is precisely the same property for $\kappa(a) = 0/1$. Hence the kernel of $\overline{\kappa}$ is just

$$\mathrm{kn}(\overline{\kappa}) \;=\; U^{-1}(\mathrm{kn}(\kappa)) \;=\; \left\{ \frac{a}{u} \;\middle|\; a \in \mathrm{kn}(\kappa), u \in U \right\}$$

(2.122) Definition: (viz. 1086)
Let $(R, +, \cdot)$ be a commutative ring, $U \subseteq R$ be a multiplicatively closed set and denote the canonical homomorphism, by $\kappa : R \to U^{-1}R : a \mapsto a/1$ again. If now $\mathfrak{a} \trianglelefteq_\mathrm{i} R$ and $\mathfrak{u} \trianglelefteq_\mathrm{i} U^{-1}R$ are ideals then we define the transferred ideals $\mathfrak{u} \cap R \trianglelefteq_\mathrm{i} R$ and $U^{-1}\mathfrak{a} \trianglelefteq_\mathrm{i} U^{-1}R$ to be the following

$$\begin{aligned} \mathfrak{u} \cap R \;&:=\; \kappa^{-1}(\mathfrak{u}) \;=\; \left\{ a \in R \;\middle|\; \frac{a}{1} \in \mathfrak{u} \right\} \\ U^{-1}\mathfrak{a} \;&:=\; \langle \kappa(\mathfrak{a}) \rangle_\mathrm{i} \;=\; \left\{ \frac{a}{u} \;\middle|\; a \in \mathfrak{a}, u \in U \right\} \end{aligned}$$

(2.123) Example:
Let $(R,+,\cdot)$ be any commutative ring, $a \in R$ and $U \subseteq R$ be multiplicatively closed. Then an easy, straightforward computation shows the identity of the principal ideals

$$U^{-1}(aR) \;=\; \frac{a}{1}\,U^{-1}R$$

(2.124) Definition: (viz. 1086)
Let $(R,+,\cdot)$ be a commutative ring, $U \subseteq R$ be a multiplicatively closed set and $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be an ideal of R. Then we obtain another ideal $\mathfrak{a} : U \trianglelefteq_{\mathrm{i}} R$ by letting

$$\mathfrak{a} : U \;:=\; \{\, b \in R \mid \exists\, v \in U : vb \in \mathfrak{a} \,\}$$

And clearly $\mathfrak{a} : U \trianglelefteq_{\mathrm{i}} R$ thereby is an ideal of R containing $\mathfrak{a} \subseteq \mathfrak{a} : U$ and using the notation of (2.122) we finally obtain the equality

$$\left(U^{-1}\mathfrak{a}\right) \cap R \;=\; \mathfrak{a} : U$$

(2.125) Proposition: (viz. 1087)
Let $(R,+,\cdot)$ be a commutative ring and $U \subseteq R$ be a multiplicatively closed subset. Further let $\mathfrak{a}, \mathfrak{b} \trianglelefteq_{\mathrm{i}} R$ be any two ideals of R, then we obtain

$$\begin{aligned}
U^{-1}(\mathfrak{a} \cap \mathfrak{b}) &= \left(U^{-1}\mathfrak{a}\right) \cap \left(U^{-1}\mathfrak{b}\right) \\
U^{-1}(\mathfrak{a} + \mathfrak{b}) &= \left(U^{-1}\mathfrak{a}\right) + \left(U^{-1}\mathfrak{b}\right) \\
U^{-1}(\mathfrak{a}\,\mathfrak{b}) &= \left(U^{-1}\mathfrak{a}\right)\left(U^{-1}\mathfrak{b}\right) \\
U^{-1}\sqrt{\mathfrak{a}} &= \sqrt{U^{-1}\mathfrak{a}}
\end{aligned}$$

$$\begin{aligned}
(\mathfrak{a} : U) : U &= \mathfrak{a} : U \\
(\mathfrak{a} \cap \mathfrak{b}) : U &= (\mathfrak{a} : U) \cap (\mathfrak{b} : U) \\
\sqrt{\mathfrak{a}} : U &= \sqrt{\mathfrak{a} : U}
\end{aligned}$$

Conversely consider any two ideals $\mathfrak{u}, \mathfrak{w} \trianglelefteq_{\mathrm{i}} U^{-1}R$ and abbreviate $\mathfrak{a} := \mathfrak{u} \cap R$ and $\mathfrak{b} := \mathfrak{w} \cap R \trianglelefteq_{\mathrm{i}} R$. Then we likewise get the additional identities

$$\begin{aligned}
(\mathfrak{u} \cap \mathfrak{w}) \cap R &= \mathfrak{a} \cap \mathfrak{b} \\
(\mathfrak{u} + \mathfrak{w}) \cap R &= (\mathfrak{a} + \mathfrak{b}) : U \\
(\mathfrak{u}\,\mathfrak{w}) \cap R &= (\mathfrak{a}\,\mathfrak{b}) : U \\
\sqrt{\mathfrak{u}} \cap R &= \sqrt{\mathfrak{a}}
\end{aligned}$$

(2.126) Example:
The equality $(\mathfrak{a} + \mathfrak{b}) : U = (\mathfrak{a} : U) + (\mathfrak{b} : U)$ need *not* hold true. As a counter-example consider $R = \mathbb{Z}$, $U := \{1, 2, 4, 8, \ldots\}$, $\mathfrak{a} = 9\mathbb{Z}$ and $\mathfrak{b} = 15\mathbb{Z}$. Then it is clear that $\mathfrak{a} : U = \mathfrak{a}$ and $\mathfrak{b} : U = \mathfrak{b}$ such that $(\mathfrak{a} : U) + (\mathfrak{b} : U) = 3\mathbb{Z}$ (as 3 is the greatest common divisor of 9 and 15). Yet $13 \cdot 2 = 26 = 9 + 15 \in \mathfrak{a} + \mathfrak{b}$. Thus $13 \in (\mathfrak{a} + \mathfrak{b}) : U$ even though $13 \notin 3\mathbb{Z} = (\mathfrak{a} : U) + (\mathfrak{b} : U)$.

(2.127) Proposition: (viz. 1088)
Let $(R,+,\cdot)$ be a commutative ring, $U \subseteq R$ be a multiplicatively closed subset and $I \neq \emptyset$ a non-empty index set. Suppose for any $i \in I$ we have an ideal $\mathfrak{a}_i \trianglelefteq_{\mathrm{i}} R$, then we get the following inclusion

$$U^{-1}\left(\bigcap_{i\in I}\mathfrak{a}_i\right) \quad\subseteq\quad \bigcap_{i\in I}\left(U^{-1}\mathfrak{a}_i\right)$$

And if for any $i \in I$ we even have a prime ideal $\mathfrak{p}_i \trianglelefteq_{\mathrm{i}} R$ with $\mathfrak{p}_i \cap U = \emptyset$ and an arbitrary ideal $\mathfrak{u}_i \trianglelefteq_{\mathrm{i}} U^{-1}R$ then we find the following identities: Nota Part of this proposition will be generalized to the transfer of ideals in general ring extensions in (8.21).

$$\begin{aligned} U^{-1}\left(\bigcap_{i\in I}\mathfrak{p}_i\right) &= \bigcap_{i\in I}\left(U^{-1}\mathfrak{p}_i\right) \\ \left(\bigcap_{i\in I}\mathfrak{u}_i\right)\cap R &= \bigcap_{i\in I}\left(\mathfrak{u}_i\cap R\right) \end{aligned}$$

(2.128) Definition: (viz. 1089)
Let $(R,+,\cdot)$ be a commutative ring and $U \subseteq R$ be a multiplicatively closed set in R. Then we define the following sets of ideals in R

$$\begin{aligned} U^{-1}\big(\mathsf{Ideal}(R)\big) &:= \{\,\mathfrak{a}\in\mathsf{Ideal}(R)\mid \mathfrak{a}=\mathfrak{a}:U\,\} \\ &= \left\{\,\mathfrak{a}\in\mathsf{Ideal}(R)\;\middle|\;\begin{array}{l}\forall\, a\in R \text{ we get the implication}\\ \big(\exists\, u\in U : ua\in\mathfrak{a}\big)\implies a\in\mathfrak{a}\end{array}\right\} \\ U^{-1}\big(\mathsf{Srad}(R)\big) &:= \mathsf{Srad}(R)\cap U^{-1}\big(\mathsf{Ideal}(R)\big) \\ U^{-1}\big(\mathsf{Spec}(R)\big) &:= \mathsf{Spec}(R)\cap U^{-1}\big(\mathsf{Ideal}(R)\big) \\ &= \{\,\mathfrak{p}\in\mathsf{Spec}(R)\mid \mathfrak{p}\cap U=\emptyset\,\} \\ U^{-1}\big(\mathsf{Smax}(R)\big) &:= \{\,\mathfrak{a}\in\mathsf{Ideal}(R)\mid \mathfrak{a}\cap U=\emptyset\,\}^{*} \end{aligned}$$

Nota explicitly an ideal $\mathfrak{m}$ of R is contained in $U^{-1}\mathsf{Smax}(R)$ iff it satisfies (1) $\mathfrak{m} \subseteq R\setminus U$ and (2) for any other $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ we have the implication $\mathfrak{m}\subseteq\mathfrak{a}\subseteq R\setminus U \implies \mathfrak{m}=\mathfrak{a}$.

(2.129) Proposition: (viz. 1089)
Let $(R,+,\cdot)$ be a commutative ring and $U \subseteq R$ be a multiplicatively closed set in R. Then we obtain an order-preserving one-to-one correspondence between the ideals of the localization $U^{-1}R$ and $U^{-1}\mathsf{Ideal}(R)$, formally this is

$$\begin{aligned} \mathsf{Ideal}(U^{-1}R) &\longleftrightarrow U^{-1}\big(\mathsf{Ideal}(R)\big) \\ \mathfrak{u} &\mapsto \mathfrak{u}\cap R \\ U^{-1}\mathfrak{a} &\hookleftarrow \mathfrak{a} \end{aligned}$$

- This correspondence is order-preserving, that is for any two ideals $\mathfrak{a}, \mathfrak{b} \in U^{-1}\mathrm{Ideal}(R)$ respectively for $\mathfrak{u}, \mathfrak{w} \in \mathrm{Ideal}U^{-1}R$ we find the implications

$$\begin{aligned} \mathfrak{a} \subseteq \mathfrak{b} &\implies U^{-1}\mathfrak{a} \subseteq U^{-1}\mathfrak{b} \\ \mathfrak{u} \subseteq \mathfrak{w} &\implies \mathfrak{u} \cap R \subseteq \mathfrak{w} \cap R \end{aligned}$$

- And this correspondence correlates maximal, prime and radical ideals of $U^{-1}R$ with $U^{-1}\mathrm{Smax}(R)$, $U^{-1}\mathrm{Spec}(R)$ respectively with $U^{-1}\mathrm{Srad}(R)$

$$\begin{array}{rcl} \mathrm{Ideal}\big(U^{-1}R\big) & \longleftrightarrow & U^{-1}\big(\mathrm{Ideal}(R)\big) \\ \cup & & \cup \\ \mathrm{Srad}\big(U^{-1}R\big) & \longleftrightarrow & U^{-1}\big(\mathrm{Srad}(R)\big) \\ \cup & & \cup \\ \mathrm{Spec}\big(U^{-1}R\big) & \longleftrightarrow & U^{-1}\big(\mathrm{Spec}(R)\big) \\ \cup & & \cup \\ \mathrm{Smax}\big(U^{-1}R\big) & \longleftrightarrow & U^{-1}\big(\mathrm{Smax}(R)\big) \end{array}$$

(2.130) Example:

- Thus the ideal structure of $U^{-1}R$ is simpler than that of R itself. The most drastic example is the following: $\mathbb{Z}$ has a multitude of ideals (namely all $a\mathbb{Z}$ where $a \in \mathbb{N}$, which are countably many). Yet $\mathbb{Q} = \mathrm{QUOT}(\mathbb{Z})$ if a field and hence only has the trivial ideals 0 and $\mathbb{Q}$ itself.

- Let now $(R, +, \cdot)$ be any commutative ring and choose any $u \in R$, then the spectrum of R_u corresponds (under the mapping $\mathfrak{u} \mapsto \mathfrak{u} \cap R$ of the proposition above) to the following subset of the spectrum of R. In (2.172.(vi)) we will also prove the likewise inclusion of the maximal ideals

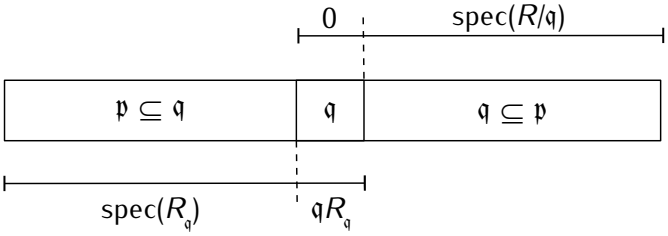
$$\begin{array}{rcl} \mathrm{Spec}\big(R_u\big) & \longleftrightarrow & \{\, \mathfrak{p} \in \mathrm{Spec}(R) \mid u \notin \mathfrak{p} \,\} \\ \cup & & \cup \\ \mathrm{Smax}\big(R_u\big) & \longleftrightarrow & \{\, \mathfrak{b} \in \mathrm{Ideal}(R) \mid u \notin \mathfrak{b} \,\}^* \end{array}$$

 Prob For a prime ideal $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ the property $u \in \mathfrak{p}$ is equivalent, to $\{\, u, u^2, u^3, \dots \,\} \subseteq \mathfrak{p}$. But this again is equivalent, to $\mathfrak{p} \cap \{\, u, u^2, u^3, \dots \,\} \neq \emptyset$ such that the claim is immediate from (2.129).

- Let $\mathfrak{q} \in \mathrm{Spec}(R)$ be a fixed prime ideal of R, then (for any other prime ideal $\mathfrak{p}$ of R) clearly $\mathfrak{p} \cap (R \setminus \mathfrak{q}) = \emptyset$ is equivalent to $\mathfrak{p} \subseteq \mathfrak{q}$. Using this in the above proposition (2.129) we find the correspondence

$$\mathrm{Spec}(R_{\mathfrak{q}}) \longleftrightarrow \{\, \mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \subseteq \mathfrak{q} \,\}$$

 Thus localizing in $\mathfrak{q}$ simply preserves the prime ideals below $\mathfrak{q}$ and deletes all the prime ideals beyond $\mathfrak{q}$. Note that this is just the opposite of the quotient $R/\mathfrak{q}$ - here all the ideals below $\mathfrak{q}$ are cut off. That is let $\mathcal{P} := \{\, \mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \subseteq \mathfrak{q} \text{ or } \mathfrak{q} \subseteq \mathfrak{p} \,\}$ be the set of all prime ideals of R comparable with $\mathfrak{q}$. Then the situation can be illustrated in the following way:



(2.131) Corollary: (viz. 1093)
Let $(R,+,\cdot)$ be a commutative ring and $U \subseteq R$ be a multiplicatively closed subset with $0 \notin U$. Further let us abbreviate by $\star$ any one of the words *integral domain*, *noetherian ring*, *artinian ring*, *UFD*, *PID*, *DKD* or *normal ring*. Then we get the following implication

$$R \text{ is a } \star \quad \Longrightarrow \quad U^{-1}R \text{ is a } \star$$

(2.132) Proposition: (viz. 1090)
Let $(R,+,\cdot)$ be any commutative ring, then we present a couple of useful isomorphies concerning localizations: Fix a multiplicatively closed set $U \subseteq R$ and some point $u \in R$ then we obtain

(i) Nota we will formulate and prove this statement for general polynomial rings $R[t \mid A]$, which will be introduced in (7.10). If you are not familiar with the general concept yet, it suffices to take $R[t \mid A] = R[t]$ of the polynomial ring $R[t]$ (which is the case $A = \mathbb{N}$) for now.

Localisation commutes with going to the polynomial ring: I.e. fix any commutative monoid A and regard the polynomial ring $R[t \mid A]$. Then we find the following isomorphism

$$\begin{array}{rcl} U^{-1}\big(R[t \mid A]\big) & \cong_{\mathrm{r}} & \big(U^{-1}R\big)[t \mid A] \\ \dfrac{f}{u} & \mapsto & \displaystyle\sum_{\alpha \in A} \frac{f[\alpha]}{u} t^{\alpha} \end{array}$$

(ii) Consider $U \subseteq R$ multiplicatively closed and $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ any ideal of R such that $U \cap \mathfrak{a} = \emptyset$. Now denote $U/\mathfrak{a} := \{\, u + \mathfrak{a} \mid u \in U \,\}$, then we obtain the following isomorphism

$$\begin{array}{rcl} U^{-1}R \,\big/\, U^{-1}\mathfrak{a} & \cong_{\mathrm{r}} & \Big(U \,\big/\, \mathfrak{a}\Big)^{-1} \Big(R \,\big/\, \mathfrak{a}\Big) \\ \dfrac{b}{v} + U^{-1}\mathfrak{a} & \mapsto & \dfrac{b+\mathfrak{a}}{v+\mathfrak{a}} \end{array}$$

(iii) The localized ring R_u can be gained by picking up a solution t to the equation $ut - 1 = 0$. That is it is just the quotient of the polynomial ring of R by $ut - 1$

$$\begin{array}{rcl} R_u & \cong_{\mathrm{r}} & R[t] \,\big/\, (ut-1)R[t] \\ \dfrac{a}{u^k} & \mapsto & at^k + (ut-1)R[t] \\ f(1/u) & \hookleftarrow & f + (ut-1)R[t] \end{array}$$

(iv) Let $(R,+,\cdot)$ be an integral domain and $0 \notin U \subseteq R$ be a multiplicatively closed subset of R *not* containing 0. Then the quotient fields of R and $U^{-1}R$ are isomorphic under

$$\text{QUOT}(R) \;\cong_{\text{r}}\; \text{QUOT}(U^{-1}R) \;:\; \frac{a}{b} \mapsto \frac{a/1}{b/1}$$

(v) Let $(R,+,\cdot)$ be an integral domain and $0 \neq a, b \in R$ be two non-zero elements of R and let $n \in \mathbb{N}$. Then we obtain the following isomorphism

$$\left(R_a\right)_{b/a^n} \;\cong_{\text{r}}\; R_{ab} \;:\; \frac{x/a^i}{(b/a^n)^j} \mapsto \frac{xa^{(n+1)j}b^i}{(ab)^{i+j}}$$

(vi) In particular: Let $\mathfrak{p} \trianglelefteq_{\text{i}} R$ be a prime ideal and $\mathfrak{a} \trianglelefteq_{\text{i}} R$ be any ideal of R such that $\mathfrak{a} \subseteq \mathfrak{p}$. Then we denote $\mathfrak{a}_\mathfrak{p} := (R \setminus \mathfrak{p})^{-1}\mathfrak{a}$ and thereby obtain the following isomorphy

$$R_\mathfrak{p} \Big/ \mathfrak{a}_\mathfrak{p} \;\cong_{\text{r}}\; \left(R \Big/ \mathfrak{a}\right)_{\mathfrak{p}/\mathfrak{a}} \;:\; \frac{b}{u} + \mathfrak{a}_\mathfrak{p} \mapsto \frac{b+\mathfrak{a}}{u+\mathfrak{a}}$$

(vii) Let $\mathfrak{p} \trianglelefteq_{\text{i}} R$ be a prime ideal of R and denote $\overline{\mathfrak{p}} := (R \setminus \mathfrak{p})^{-1}\mathfrak{p}$. If now $a \notin \mathfrak{p}$ is *not* contained in $\mathfrak{p}$ then we obtain the isomorphy

$$R_\mathfrak{p} \;\cong_{\text{r}}\; (R_a)_{\overline{\mathfrak{p}}} \;:\; \frac{a}{u} \;\mapsto\; \frac{r/1}{u/1}$$

(2.133) Lemma: (viz. 1083)
Local-Global-Principle: Let $(R,+,\cdot)$ be any commutative ring and $a, b \in R$, then we obtain the equivalence of the following statements

$$\begin{aligned} a = b \quad &\iff \quad \forall\, \mathfrak{p} \in \text{Spec}(R) \;:\; \frac{a}{1} = \frac{b}{1} \in R_\mathfrak{p} \\ &\iff \quad \forall\, \mathfrak{m} \in \text{Smax}(R) \;:\; \frac{a}{1} = \frac{b}{1} \in R_\mathfrak{m} \end{aligned}$$

Further if R is an integral domain and $F := \text{QUOT}(R)$ is its quotient field, then we can embed R into F, as $R = \{\, a/1 \in F \mid a \in R \,\}$. Likewise if $\mathfrak{p} \trianglelefteq_{\text{i}} R$ is a prime ideal then we embed the localization into the quotient field F as well, in the form $R_\mathfrak{p} = \{\, a/u \in F \mid a \in R,\; u \notin \mathfrak{p} \,\}$. And thereby we obtain the following identities (as subsets of F)

$$R \;=\; \bigcap_{\mathfrak{p} \in \text{spec}R} R_\mathfrak{p} \;=\; \bigcap_{\mathfrak{m} \in \text{smax}R} R_\mathfrak{m}$$

(2.134) Corollary: (viz. 1100)
Let $(R,+,\cdot)$ be an integral domain and denote its quotient field by $E := \text{QUOT}(R)$. Then the following three statements are equivalent

(a) R is normal

(b) $\forall\, \mathfrak{p} \in \text{Spec}(R) \;:\; R_\mathfrak{p}$ is normal

(c) $\forall\, \mathfrak{m} \in \text{Smax}(R) \;:\; R_\mathfrak{m}$ is normal

2.11 Local Rings

Not surprisingly a local ring is the result of localizing a commutative ring (in a prime ideal). These rings only have a single maximal ideal and this has several very restrictive consequences: Local rings have a very orderly structure. We will also see that external functions (valuations) may also enforce powerful restrictions on the rings internal structure, only allowing local rings.

(2.135) Definition: (viz. 1103)
Let $(R,+,\cdot)$ be any commutative ring, then R is said to be a **local ring**, iff it satisfies one of the following two equivalent properties

(a) R has precisely one maximal ideal (i.e. $\#\operatorname{Smax}(R) = 1$)

(b) the set of non-units is an ideal $R \setminus R^* \trianglelefteq_{\mathrm{i}} R$ in R

Nota In this case the uniquely determined maximal ideal of R is precisely the set of non-units $R \setminus R^*$, which can always be given explicitly as $R \setminus R^* = \{a \in R \mid aR \neq R\} \trianglelefteq_{\mathrm{i}} R$.

(2.136) Proposition: (viz. 1103)
Let $(R,+,\cdot)$ be a commutative ring and $\mathfrak{m} \trianglelefteq_{\mathrm{i}} R$ be a proper ideal of R (that is $\mathfrak{m} \neq R$). Then the following four statements are equivalent

(a) R is a local ring with maximal ideal $\mathfrak{m}$

(b) $\forall\, \mathfrak{a} \trianglelefteq_{\mathrm{i}} R \,:\, \mathfrak{a} \neq R \implies \mathfrak{a} \subseteq \mathfrak{m}$

(c) $R \setminus \mathfrak{m} = R^*$

(d) $R \setminus \mathfrak{m} \subseteq R^*$

(2.137) Example:

- If $(F,+,\cdot)$ is a field, then $F \setminus \{0\} = F^*$, in particular F already is a local ring having the maximal ideal $\{0\}$. And of course the converse is true, as well: If $\{0\}$ is a maximal ideal in the commutative ring F, then F is a field.
- Let $(E,+,\cdot)$ be a field and consider the ring of formal power series $R := E[\![t]\!]$ over E. Then $E[\![t]\!]$ is a local ring having the maximal ideal

$$\mathfrak{m} \;:=\; t\,E[\![t]\!] \;=\; \{\, f \in E[\![t]\!] \mid f[0] = 0 \,\}$$

 To prove this it suffices to check $R \setminus \mathfrak{m} \subseteq R^*$ (due to the above proposition (2.136)). But in fact if $f \in E[\![t]\!]$ is any power series with $f[0] \neq 0$ then an elementary computation shows that we can iteratively compute the inverse of f, by

$$\begin{aligned} f^{-1}[0] &= \frac{1}{f[0]} \\ f^{-1}[k] &= \frac{-1}{f[0]} \sum_{j=0}^{k-1} f[k-j] f^{-1}[j] \end{aligned}$$

- Let $(R,+,\cdot)$ be a commutative ring and $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ be any prime ideal of R. Then in (2.138) below we will prove that the localized ring $R_{\mathfrak{p}}$ is a local ring having the maximal ideal

$$\mathfrak{m}_{\mathfrak{p}} \;:=\; (R \setminus \mathfrak{p})^{-1}\mathfrak{p} \;=\; \{\, p/u \mid p \in \mathfrak{p}, u \notin \mathfrak{p} \,\}$$

- If $(R,+,\cdot)$ is a local ring with maximal ideal $\mathfrak{m}$ and $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ is a proper ideal of R, then the quotient ring $R/\mathfrak{a}$ is a local ring again, with maximal ideal $\mathfrak{m}/\mathfrak{a}$.

 Prob as $\mathfrak{a} \neq R$ we have $\mathfrak{a} \subseteq \mathfrak{m}$, there is a maximal ideal containing $\mathfrak{a}$ by (2.4.(ii)) and $\mathfrak{m}$ is the only maximal ideal, available. Also $\mathrm{Smax}(R/\mathfrak{a})$ corresponds to $\{\, \mathfrak{m} \in \mathrm{Smax}(R) \mid \mathfrak{a} \subseteq \mathfrak{m} \,\} = \{\, \mathfrak{m} \,\}$, according to (1.71). Thus $\mathfrak{m}/\mathfrak{a}$ is the one and only maximal ideal of $R/\mathfrak{a}$.

- Let $(S,+,\cdot)$ be a PID, $1 \leq n \in \mathbb{N}$ and $p \in S$ be a prime element of S. Then we have proved in (2.109.(iii)) that $R := S/p^nS$ is a local ring having the maximal ideal

$$\mathrm{NIL}(R) \;=\; \mathrm{ZD}(R) \;=\; R \setminus R^* \;=\; (p + p^nS)\,R$$

- If $(R,+,\cdot)$ is any commutative ring and $\mathfrak{m} \trianglelefteq_{\mathrm{i}} R$ is a maximal ideal of R, then for any power $1 \leq n \in \mathbb{N}$ the ring $S := R/\mathfrak{m}^n$ is local, having the maximal ideal $\mathfrak{m}/\mathfrak{m}^n$.

 Prob Let $\overline{\mathfrak{n}} \trianglelefteq_{\mathrm{i}} S$ be any maximal ideal of S, then this is of the form $\overline{\mathfrak{n}} = \mathfrak{n}/\mathfrak{m}^n$ for some maximal ideal $\mathfrak{n}$ of R with $\mathfrak{m}^n \subseteq \mathfrak{n}$. But as $\mathfrak{n}$ also is prime this implies $\mathfrak{m} \subseteq \mathfrak{n}$ and hence $\mathfrak{n} = \mathfrak{m}$, since $\mathfrak{m}$ is maximal in R, too. Hence the maximal ideal of S is uniquely determined.

- A local ring need not be noetherian: As an example consider the polynomial ring in infinitely many variables $R = E[t_1, t_2, \ldots]$ over a field $(E,+,\cdot)$ and the maximal ideal $\mathfrak{m} := \langle t_1, t_2, \ldots \rangle_{\mathrm{i}} \trianglelefteq_{\mathrm{i}} R$. Then the localization $R_{\mathfrak{m}}$ of R in $\mathfrak{m}$ is a local ring with maximal ideal $\mathfrak{m}R_{\mathfrak{m}}$. According to (2.129) it also contains an infinitely ascending chain of prime ideals however

$$\langle t_1 \rangle_{\mathrm{i}} R_{\mathfrak{m}} \;\subset\; \langle t_1, t_2 \rangle_{\mathrm{i}} R_{\mathfrak{m}} \;\subset\; \langle t_1, t_2, t_3 \rangle_{\mathrm{i}} R_{\mathfrak{m}} \;\subset\; \ldots$$

(2.138) Proposition: (viz. 1103)
Let $(R,+,\cdot)$ be a commutative ring and consider a set $\mathcal{Q} = \{\, \mathfrak{q}_1, \ldots, \mathfrak{q}_n \,\} \subseteq \mathrm{Spec}(R)$ of finitely many prime ideals of R. Let $Q := \mathfrak{q}_1 \cup \cdots \cup \mathfrak{q}_n \subseteq R$ be the union of these ideals and let

$$U \;:=\; R \setminus Q \;=\; \bigcap_{i=1}^{n} (R \setminus \mathfrak{q}_i)$$

Then $U \subseteq R$ is multiplicatively closed such that we can localize $U^{-1}R$. Recall that any ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ with $\mathfrak{a} \cap U = \emptyset$ (that is $\mathfrak{a} \subseteq R \setminus P$) corresponds to an ideal

$$\mathfrak{a}\,U^{-1}R \;=\; U^{-1}\mathfrak{a} \;=\; \left\{ \frac{a}{u} \mid a \in \mathfrak{a}, u \in U \right\}$$

of $U^{-1}R$. Now denote the set of all ideals maximal in $\mathcal{Q}$ by $\mathcal{Q}^*$. That is $\mathfrak{m} \in \mathcal{Q}^*$ if and only if $\mathfrak{m} \in \mathcal{Q}$ and for any $\mathfrak{q} \in \mathcal{Q}$ we get $\mathfrak{m} \subseteq \mathfrak{q} \implies \mathfrak{m} = \mathfrak{q}$. Then we can explicitly give the prime and maximal ideals of $U^{-1}R$ to be the following

$$\begin{aligned} \operatorname{Spec}(U^{-1}R) &= \left\{ U^{-1}\mathfrak{p} \;\middle|\; \begin{array}{l} \mathfrak{p} \in \operatorname{Spec}(R) \text{ such that} \\ \exists\, \mathfrak{m} \in \mathcal{Q}^* : \mathfrak{p} \subseteq \mathfrak{m} \end{array} \right\} \\ \operatorname{Smax}(U^{-1}R) &= \left\{ U^{-1}\mathfrak{m} \mid \mathfrak{m} \in \mathcal{Q}^* \right\} \end{aligned}$$

In particular $U^{-1}R$ has finitely many maximal ideals only (such a ring is called *semi-local*). In case $n = 1$, that is $\mathcal{Q} = \{ \mathfrak{p} \}$, of a single prime ideal $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ the ring $R_{\mathfrak{p}} := (R \setminus \mathfrak{p})^{-1}R$ only has one maximal ideal (such a ring is called *local*). Thereby the maximal ideal of $R_{\mathfrak{p}}$ is given to be

$$\mathfrak{m}_{\mathfrak{p}} := (R \setminus \mathfrak{p})^{-1}\mathfrak{p} = \left\{ \frac{p}{u} \mid p \in \mathfrak{p},\, u \in R \setminus \mathfrak{p} \right\}$$

And the residue field of $R_{\mathfrak{p}}$ modulo $\mathfrak{m}_{\mathfrak{p}}$ is isomorphic to the quotient field of $R/\mathfrak{p}$ under the isomorphism

$$R_{\mathfrak{p}} \Big/ \mathfrak{m}_{\mathfrak{p}} \cong_{\mathrm{f}} \operatorname{QUOT}\left(R \Big/ \mathfrak{p} \right) : \frac{a}{u} + \mathfrak{m}_{\mathfrak{p}} \mapsto \frac{a + \mathfrak{p}}{u + \mathfrak{p}}$$

(2.139) Proposition: (viz. 1104)
Let $(R, +, \cdot)$ be a local ring with maximal ideal $\mathfrak{m}$ and let $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be any ideal of R. Then the following four statements are equivalent

(a) $\sqrt{\mathfrak{a}} = \mathfrak{m}$

(b) $\mathfrak{a}$ is $\mathfrak{m}$-primary

(c) $\mathfrak{m}$ is a minimal prime ideal over $\mathfrak{a}$

(d) $\mathfrak{m}$ is the only prime ideal containing $\mathfrak{a}$, i.e. $\mathbb{V}(\mathfrak{a}) = \{ \mathfrak{m} \}$

Discrete Valuation Rings

(2.140) Definition:
Let $(R, +, \cdot)$ be any non-zero (i.e. $R \neq 0$), commutative ring, then a mapping $\nu : R \to \mathbb{N} \cup \{\infty\}$ is said to be a **valuation** (and the ordered pair (R, ν) a **valued ring**) iff for any $a, b \in R$ we obtain the following three properties

(1) $\nu(a) = \infty \iff a = 0$

(2) $\nu(ab) = \nu(a) + \nu(b)$

(3) $\nu(a + b) \geq \min\{ \nu(a), \nu(b) \}$

And a valuation ν is said to be **normed** iff it further satisfies the following fourth property

(N) $\exists\, a \in R : \nu(a) = 1$

(2.141) Remark:
So what is the connection between local rings and valuations? In fact, it is readily apparent that the maximal ideal $\mathfrak{m}$ of a local ring R constitutes a map ν of the form $\nu : R \to \mathbb{N} \cup \{\infty\}$, that inspired the definition of a valuation, namely

$$\nu(a) \;:=\; \sup\{k \in \mathbb{N} \mid a \in \mathfrak{m}^k\}$$

This map satisfies $\nu(0) = \infty$, $\nu(ab) \geq \nu(a) + \nu(b)$ and $\nu(a+b) \geq \min\{\nu(a), \nu(b)\}$ for any ideal $\mathfrak{m}$. In a local ring we also have $R^* = [\nu] := \{a \in R \mid \nu(a) = 0\}$. In general ν need not be a valuation, we will require further properties for this.

Prob Clearly $0 \in \mathfrak{m}^k$ for any $k \in \mathbb{N}$ and hence $\nu(0) = \infty$. Also if $\nu(a) = j$ and $\nu(b) = k$ then $a \in \mathfrak{m}^j$ and $b \in \mathfrak{m}^k$ and therefore $ab \in \mathfrak{m}^{j+k}$ which is $\nu(ab) \geq j + k$. Without loss of generality assume $j \leq k$, then $b \in \mathfrak{m}^k \subseteq \mathfrak{m}^j$ and hence $a + b \in \mathfrak{m}^j$ again, hence $\nu(a+b) \geq j$. Finally $\nu(a) = 0$ iff $a \in R \setminus \mathfrak{m} = R^*$.

(2.142) Proposition: (viz. 1104)

(i) Let (R, ν) be a valued ring (in particular $R \neq 0$), then R and its valuation ν already satisfy the following additional properties

(U) $a \in R^* \implies \nu(a) = 0$

(I) R is an integral domain

(P) $[\nu] := \{a \in R \mid \nu(a) \geq 1\} \in \mathrm{Spec}(R)$

(ii) If $(R, +, \cdot)$ is a non-zero integral domain then R always carries the **trivial valuation** which we denote by $\tau : R \to \mathbb{N} \cup \{\infty\}$ and which is defined by $\tau(a) := 0$ iff $a \neq 0$ and $\tau(a) := \infty$ iff $a = 0$. Note that this valuation is *not* normed, of course.

(iii) Let $(R, +, \cdot)$ be a noetherian integral domain and consider any $p \in R$ prime. Then we obtain a normed valuation $\nu = \nu_p$ on R that satisfies $\nu(p) = 1$ and $[\nu] = pR$, by letting

$$\nu \;:\; R \to \mathbb{N} \cup \{\infty\} \;:\; a \mapsto [a]_p$$

$$\text{where} \quad [a]_p \;:=\; \sup\Big\{ k \in \mathbb{N} \mid p^k \mid a \Big\}$$

And for any $a, b \in R$ this valuation satisfies a fifth property, namely we also get the implication

$$\nu(a) \neq \nu(b) \quad \Longrightarrow \quad \nu(a+b) = \min\{\nu(a), \nu(b)\}$$

(iv) Let $(R, +, \cdot)$ be a PID then we obtain a one-to-one correspondence between the maximal spectrum of R and the normed valuations on R, using the construction in (iii)

$$\begin{array}{rcl} \mathrm{Smax}(R) & \longleftrightarrow & \{\nu : R \to \mathbb{N} \cup \{\infty\} \mid (1), (2), (3), (N)\} \\ \mathfrak{m} & \mapsto & \nu_p \text{ where } \mathfrak{m} = pR \\ [\nu] & \hookleftarrow & \nu \end{array}$$

(2.143) Remark:
In a polynomial ring, do not confuse valuations with degrees. E.g. in the polynomial ring $R = \mathbb{Z}[t]$ the degree is the highest power $\deg(f) = n$ occurring in the polynomial $f(t) = a_n t^n + \cdots + a_1 t + a_0$. Hence the degree is bounded from above $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$.
Taking to $p = t \in R$ the valuation ν_t is the lowest power occurring in a polynomial f. That is: If $f \in R[t]$ is of the form $f(t) = a_n t^n + \cdots + a_m t^m$ with $a_n \neq 0$ and $a_m \neq 0$, but all coefficients $f[k] = 0$ for $k \notin m \ldots n$, then $\deg(f) = n$ and $\nu_t(f) = m$. Therefore the valuation ν_t is bounded from below $\nu_t(f+g) \geq \min\{\nu_t(f), \nu_t(g)\}$. So generally speaking the one and only common property of degrees and valuations is multiplicativity. Apart from that they are similar but separate concepts.

(2.144) Definition:
Let $(R, +, \cdot)$ be a commutative ring, then we call $\nu : R \to \mathbb{N} \cup \{\infty\}$ a **discrete valuation** on R (and the ordered pair (R, ν) is said to be a **discrete valuation ring**), iff ν satisfies all of the following properties (for any a, $b \in R$)

(1) $\nu(a) = \infty \iff a = 0$

(2) $\nu(ab) = \nu(a) + \nu(b)$

(3) $\nu(a+b) \geq \min\{\nu(a), \nu(b)\}$

(4) $\nu(a) \leq \nu(b) \implies a \mid b$

(N) $\exists\, m \in R : \nu(m) = 1$

(2.145) Example:

- The prototype of a discrete valuation ring is the ring of formal power series $E[\![t]\!]$ over a field E. And in this case we obtain a discrete valuation ν (note that $[\nu] = tE[\![t]\!]$), by
$$\nu : E[\![t]\!] \to \mathbb{N} \cup \{\infty\} : f \mapsto \sup\left\{ k \in \mathbb{N} \mid t^k \mid f \right\}$$
- We regard $F = \mathbb{Q}$ and fix any prime number $p \in \mathbb{Z}$. Then we obtain a discrete valuation ν_p in the sense of (2.146.(vi)) on the field $\mathbb{Q}$ by letting $\nu_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ (where a, $b \in \mathbb{Z}$, $b \neq 0$)
$$\nu_p\left(\frac{a}{b}\right) := [a]_p - [b]_p$$
$$[a]_p := \sup\left\{ k \in \mathbb{N} \mid p^k \mid a \right\}$$
Thereby ν_p is said to be the *p-adic valuation* of $\mathbb{Q}$. And if we denote $\mathfrak{p} := p\mathbb{Z}$, then the discrete valuation ring determined by ν_p is just $\{a \in \mathbb{Q} \mid \nu_p(a) \geq 0\} \cong_r \mathbb{Z}_{\mathfrak{p}}$ canonically.
- More generally the above construction works out for any PID R: Let F be the quotient field of R and $p \in R$ be any prime element. Then we may repeat the definition of ν_p literally (except for a, $b \in R$) and thereby obtain a discrete valuation $\nu_p : F \to \mathbb{Z} \cup \{\infty\}$. And the discrete valuation ring determined by ν_p is $R_{\mathfrak{p}}$ (where $\mathfrak{p} := pR$) again.

(2.146) Proposition: (viz. 1105)
Let (R,ν) be a discrete valuation ring, in particular $\nu : R \to \mathbb{N} \cup \{\infty\}$, then R and its valuation ν already satisfy all of the following additional properties

(i) (R,ν) is a valued ring, in particular R is a non-zero integral domain.

(ii) R is a local ring with maximal ideal $[\nu] = \{a \in R \mid \nu(a) \geq 1\}$.

(iii) (R,ε) is an Euclidean domain under $\varepsilon : R \setminus \{0\} \mapsto \mathbb{N} : a \mapsto \nu(a)$.

(iv) Fix any $m \in R$ with $\nu(m) = 1$, then for any $0 \neq a \in R$ there is a uniquely determined unit $\alpha \in R^*$ such that $a = \alpha m^k$ for $k = \nu(a)$.

(v) Fix any $m \in R$ with $\nu(m) = 1$ again, as R is a PID and m divides any $a \neq 0$ with $\nu(a) \geq 1$, we find that the set of ideals of R is given to be the following

$$\mathsf{Ideal}(R) \;=\; \left\{ m^k R \;\middle|\; k \in \mathbb{N} \right\} \cup \{0\}$$

(vi) Let $(F,+,\cdot)$ be an arbitrary field and $\nu : F \to \mathbb{Z} \cup \{\infty\}$ be a discrete valuation except for the void divisibility condition (4). That is ν satisfies the following four properties (for any $x, y \in F$)

(1) $\nu(x) = \infty \iff x = 0$
(2) $\nu(xy) \;=\; \nu(x) + \nu(y)$
(3) $\nu(x+y) \;\geq\; \min\{\, \nu(x), \nu(y) \,\}$
(N) $\exists\, m \in F \;:\; \nu(m) = 1$

Then we obtain a sub-ring R of F by letting $R := \{a \in F \mid \nu(a) \geq 0\} \;\leq_{\mathsf{r}}\; F$. Also $\nu : R \to \mathbb{N} \cup \{\infty\}$ is a discrete valuation on R and finally F is the quotient field of R, that is we get

$$F \;=\; \left\{ ab^{-1} \mid a,b \in F,\; b \neq 0 \right\}$$

(2.147) Theorem: (viz. 1106)
A commutative ring $(R,+,\cdot)$ is said to be a **discrete valuation ring** (abbreviated by DVR), iff it satisfies one of the following six equivalent properties

(a) R admits a discrete valuation $\nu : R \to \mathbb{N} \cup \{\infty\}$

(b) R is an integral domain and there is some element $0 \neq m \in R$ satisfying

$$R \setminus mR = R^* \quad \text{and} \quad \bigcap_{k \in \mathbb{N}} m^k R = 0$$

(c) R is a PID and local ring but not a field.

(d) R is an UFD but no field and any two prime elements of R are associates (i.e. if $p, q \in R$ are irreducible, then we get $pR = qR$).

(e) R is a noetherian integral domain and local ring, whose maximal ideal $\mathfrak{m}$ is a non-zero principal ideal (i.e. $\mathfrak{m} = mR$ for some $0 \neq m \in R$).

(f) R is a noetherian, normal and local ring with non-zero maximal ideal $\mathfrak{m} \neq 0$ and the only prime ideals of R are 0 and $\mathfrak{m}$ (i.e. $\mathrm{Spec}(R) = \{0, \mathfrak{m}\}$).

(2.148) Definition:
A commutative ring $(R, +, \cdot)$ is said to be a **valuation ring**, iff it is a non-zero integral domain in which the *divides* relation is a total order. Formally that is, iff R satisfies the following three properties

(1) $R \neq 0$

(2) R is an integral domain

(3) $\forall\, a, b \in R$ we get $a \mid b$ or $b \mid a$

(2.149) Remark:
The last property (3) in the definition above might seem a little artificial. We hence wish to explain where it comes from: As R is an integral domain we may regard its quotient field $E := \mathrm{QUOT}(R)$. Then property (3) can be reformulated, as

$$\forall\, x \in E \setminus \{0\} \quad : \quad x \in R \text{ or } x^{-1} \in R$$

Thus if we are given a valuation (in the sense of fields) $\nu : E \to \mathbb{Z} \cup \{0\}$ on E, we may regard the sub-ring $R := \{a \in E \mid \nu(a) \geq 0\}$. And it is clear that R satisfies the property $x \in R$ or $x^{-1} \in R$ for any $0 \neq x \in E$. Thus every ν is assigned a valuation ring R in E. Therefore valuation rings appear naturally whenever we regard valuations on fields.

(2.150) Corollary: (viz. 1108)

(i) If $(R, +, \cdot)$ is a valuation ring, then R already is a local ring and Bezout domain (that is any finitely generated ideal already is principal).

(ii) If $(R, +, \cdot)$ is a valuation ring, then we get the following equivalences

(a) R is noetherian

(b) R is a PID

(c) R is a DVR or field

2.12 Dedekind Domains

Prime factorization of elements of a ring (preferably an UFD) is a powerful tool in algebra, however it is available in very tame rings, such as PIDs or polynomial rings over a field. We have already studied Lasker-Noether theory of decomposition of an ideal into primary ideals. What follows is something in between: Factorization of ideals into prime ideals, just like primary decomposition of elements. Though this has somewhat nicer properties than Lasker-Noether decomposition, the price is more strict requirements of the underlying ring. In the end this is a beautiful theory that has some applications in algebraic number theory:

(2.151) Definition:
Let $(R,+,\cdot)$ be an integral domain and let us denote its quotient field by $F := \mathrm{QUOT}(R)$. Then a subset $\mathfrak{f} \subseteq F$ is called a **fraction ideal** of R (which we abbreviate by writing $\mathfrak{f} \trianglelefteq_{\mathfrak{f}} R$) iff it satisfies

(1) $\mathfrak{f} \leq_{\mathfrak{m}} F$ is an R-sub-module of F

(2) $\exists\, 0 \neq r \in R$ such that $r\mathfrak{f} \subseteq R$

(2.152) Remark:

- In particular any ideal $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$ is a fraction ideal $\mathfrak{a} \trianglelefteq_{\mathfrak{f}} R$ (Prob just let $r = 1$). By abuse of nomenclature ordinary ideals of R are hence also said to be the *integral ideals* of F.
- Conversely for any fraction ideal $\mathfrak{f} \trianglelefteq_{\mathfrak{f}} R$ we see that $\mathfrak{f} \cap R \trianglelefteq_{\mathfrak{i}} R$ is an ideal of R. Prob because $0 \in \mathfrak{f} \cap R$ and looking at some $f, g \in \mathfrak{f}$ and $a \in R$ we clearly get $f + g \in \mathfrak{f} \cap R$ and $af \in \mathfrak{f} \cap R$ as both, $\mathfrak{f}$ and R are R-modules.
- And clearly for any $x \in F$ the generated module $\mathfrak{f} := xR$ is a fraction ideal $\mathfrak{f} \trianglelefteq_{\mathfrak{f}} R$ of R Prob because if $x = r/s$ then obviously $s\mathfrak{f} = rR \subseteq R$.
- If R itself is a field, then $F = R$ and the only possible fraction ideals of R are 0 and R itself. Prob suppose there was some $x \neq 0$ such that $x \in \mathfrak{f} \trianglelefteq_{\mathfrak{f}} R$, then x has an inverse $x^{-1} \in R$ and hence $1 = x^{-1}x \in \mathfrak{f}$. Thus for any $a \in R$ we have $a = a1 \in \mathfrak{f}$.

(2.153) Proposition: (viz. 1109)
Let $(R,+,\cdot)$ be an integral domain and let us denote its quotient field by $F := \mathrm{QUOT}(R)$. As in the case of integral ideals, if $\mathfrak{f}$ and $\mathfrak{g} \trianglelefteq_{\mathfrak{f}} R$ are fraction ideals of R, then the sum $\mathfrak{f}+\mathfrak{g}$, intersection $\mathfrak{f}\cap\mathfrak{g}$ and product $\mathfrak{f}\mathfrak{g}$ of finitely many fraction ideals is a fraction ideal again. And if $\mathfrak{g} \neq 0$ we may also define the quotient $\mathfrak{f} : \mathfrak{g}$ of two fraction ideals. I.e. if $\mathfrak{f}$ and $\mathfrak{g} \trianglelefteq_{\mathfrak{f}} R$ are fraction ideals of R then we obtain further fraction ideals of R by letting

$$\begin{aligned} \mathfrak{f}+\mathfrak{g} &:= \{\, x+y \mid x \in \mathfrak{f}, y \in \mathfrak{g} \,\} \\ \mathfrak{f}\cap\mathfrak{g} &:= \{\, x \mid x \in \mathfrak{f} \text{ and } x \in \mathfrak{g} \,\} \\ \mathfrak{f}:\mathfrak{g} &:= \{\, x \in F \mid x\mathfrak{g} \subseteq \mathfrak{f} \,\} \end{aligned}$$

$$\mathfrak{f}\mathfrak{g} := \left\{ \sum_{i=1}^{n} f_i g_i \;\middle|\; n \in \mathbb{N}, f_i \in \mathfrak{f}, g_i \in \mathfrak{g} \right\}$$

(2.154) Remark:

- Let now $0 \neq \mathfrak{f}$ and $\mathfrak{g} \trianglelefteq_{\mathfrak{f}} R$ be two non-zero fraction ideals of the integral domain $(R, +, \cdot)$ and let $F = \mathrm{QUOT}(R)$. Then the product $\mathfrak{f}\mathfrak{g}$ and quotient $\mathfrak{f} : \mathfrak{g} \neq 0$ are non-zero, too. Formally that is

$$\mathfrak{f}, \mathfrak{g} \neq 0 \quad \Longrightarrow \quad \mathfrak{f}\mathfrak{g} \neq 0 \text{ and } \mathfrak{f} : \mathfrak{g} \neq 0$$

 Prob as $\mathfrak{f}$ and $\mathfrak{g} \neq 0$ we may choose some $0 \neq f \in \mathfrak{f}$ and $0 \neq g \in \mathfrak{g}$. Then $fg \in \mathfrak{f}\mathfrak{g}$ and $fg \neq 0$, as F is an integral domain (yielding $\mathfrak{f}\mathfrak{g} \neq 0$). Now let $s\,\mathfrak{g} \subseteq R$ for some $s \neq 0$. Then $(sf)\mathfrak{g} = f(s\,\mathfrak{g}) \subseteq fR \subseteq \mathfrak{f}$ and hence $sf \in \mathfrak{f} : \mathfrak{g}$. But as $sf \neq 0$ this means $\mathfrak{f} : \mathfrak{g} \neq 0$.

- For any fraction ideal $\mathfrak{f} \trianglelefteq_{\mathfrak{f}} R$ we always get the inclusions: $\mathfrak{f}(R : \mathfrak{f}) \subseteq R \subseteq \mathfrak{f} : \mathfrak{f}$.

 Prob $\mathfrak{f}(R : \mathfrak{f})$ contains elements of the form $x_1y_1 + \cdots + x_ny_n$ where $x_i \in R : \mathfrak{f}$ and $y_i \in \mathfrak{f}$. But by definition of $R : \mathfrak{f}$ this means $x_iy_i \in R$ and hence $x_1y_1 + \cdots + x_ny_n \in R$. And $R \subseteq \mathfrak{f} : \mathfrak{f}$ is clear, as $\mathfrak{f} \leq_{\mathfrak{m}} F$ such that $ay \in \mathfrak{f}$ for any $a \in R$ and $y \in \mathfrak{f}$.

- First note that the multiplication $\mathfrak{f}\mathfrak{g}$ of fraction ideals is both commutative and associative. Further it is clear that for any fraction ideal $\mathfrak{f} \trianglelefteq_{\mathfrak{f}} R$ we get $R\mathfrak{f} = \mathfrak{f}$. That is the set of fraction ideals of R is a commutative monoid under the multiplication (defined in (2.153)) with neutral element R. This naturally leads to the definition of an *invertible* fraction ideal. Of course the non-zero fraction ideals als form a monoid and this is called the *class monoid* of R, denoted by

$$\mathcal{C}(R) \;:=\; \{\, \mathfrak{f} \trianglelefteq_{\mathfrak{f}} R \mid \mathfrak{f} \neq 0 \,\}$$

(2.155) Definition: (viz. 1109)
Let $(R, +, \cdot)$ be an integral domain and let us denote its quotient field by $F := \mathrm{QUOT}(R)$. Then a fraction ideal $\mathfrak{f} \trianglelefteq_{\mathfrak{f}} R$ of R is said to be **invertible**, iff it satisfies one of the following two equivalent conditions

(a) $\exists\, \mathfrak{g} \trianglelefteq_{\mathfrak{f}} R \;:\; \mathfrak{f}\mathfrak{g} = R$

(b) $\mathfrak{f}(R : \mathfrak{f}) \;=\; R$

Note that in this case the fraction ideal $\mathfrak{g}$ with $\mathfrak{f}\mathfrak{g} = R$ is uniquely determined, to be $\mathfrak{g} = R : \mathfrak{f}$. And it is called the **inverse** of $\mathfrak{f}$, written as

$$\mathfrak{f}^{-1} \;:=\; \mathfrak{g} \;=\; R : \mathfrak{f}$$

(2.156) Proposition: (viz. 1109)
Let $(R, +, \cdot)$ be an integral domain and let us denote its quotient field by $F := \mathrm{QUOT}(R)$ again. If now $0 \neq \mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$ is a non-zero ideal of R, then the following statements are equivalent

(a) $\mathfrak{a}$ is invertible (as a fraction ideal of R), i.e. $\mathfrak{a}\,\mathfrak{g} = R$ for a suitable fraction ideal $\mathfrak{g} \trianglelefteq_{\mathfrak{f}} R$ of R.

(b) There are some $a_1, \ldots a_n \in \mathfrak{a}$ and $x_1, \ldots, x_n \in F$ such that for any $i \in 1 \ldots n$ we get $x_i\,\mathfrak{a} \subseteq R$ and $a_1x_1 + \cdots + a_nx_n = 1$.

(c) $\mathfrak{a}$ is a projective R-module, i.e. there is a free R-module M and a sub-module $P \leq_{\mathfrak{m}} M$ such that M is a direct sum featuring $\mathfrak{a} \oplus P = M$.

(2.157) Corollary: (viz. 1110)
Let $(R,+,\cdot)$ be a local ring, that also is an integral domain. If now $0 \neq \mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$ is a non-zero ideal of R then the following statements are equivalent

(a) $\mathfrak{a}$ is a principal ideal (i.e. $\mathfrak{a} = aR$ for some $a \in R$)

(b) $\mathfrak{a}$ is invertible (as a fraction ideal $\mathfrak{a} \trianglelefteq_{\mathfrak{f}} R$)

(2.158) Remark:

- If aR is any non-zero ($a \neq 0$) principal ideal in an integral domain $(R,+,\cdot)$, then $aR \trianglelefteq_{\mathfrak{f}} R$ is an invertible fraction ideal of R. This is clear as its inverse obviously given by

$$\Big(aR\Big)^{-1} \;=\; \frac{1}{a}R$$

- Now consider an (integral) ideal $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$ and elements $a_1,\ldots,a_n \in \mathfrak{a}$ and $x_1,\ldots,x_n \in R : \mathfrak{a} \subseteq F$ such that $a_1x_1 + \cdots + a_nx_n = 1$. Then $\mathfrak{a}$ is already generated by the a_i, formally that is

$$\mathfrak{a} \;=\; \langle a_1,\ldots,a_n\rangle_{\mathfrak{i}}$$

 Prob the inclusion " $\supseteq$ " is clear, as $a_i \in \mathfrak{a}$. For the converse inclusion we consider any $a \in \mathfrak{a}$. As $x_i \in R : \mathfrak{a}$ we in particular have $x_i\mathfrak{a} \subseteq R$. And because of $a_1x_1 + \cdots + a_nx_n = 1$ we are able to write a in the form $a = (x_1a)a_1 + \cdots + (x_na)a_n \in \langle a_1,\ldots,a_n\rangle_{\mathfrak{i}}$.

- We have seen in the proposition above, that an (integral) ideal $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$ is invertible if and only if there are $a_1,\ldots,a_n \in \mathfrak{a}$ and $x_1,\ldots,x_n \in F$ such that for any $i \in 1\ldots n$ we get

$$x_i\,\mathfrak{a} \in R \quad\text{and}\quad a_1x_1 + \cdots + a_nx_n = 1$$

 Nota as we have just seen this already implies, that the a_i generate $\mathfrak{a}$. Hence any invertible ideal already is finitely generated!

- Now consider some multiplicatively closed subset $0 \notin U \subseteq R$. Then $F = \textsc{quot}(R) = \textsc{quot}(U^{-1}R)$ are canonically isomorphic, by (2.132.(iii)). If now $\mathfrak{f}$ and $\mathfrak{g} \trianglelefteq_{\mathfrak{f}} R$ are any two fraction ideals of R then it is easy to see that $U^{-1}\mathfrak{f} := \{\, a/ub \mid a/b \in \mathfrak{f}, u \in U \,\} \trianglelefteq_{\mathfrak{f}} U^{-1}R$ is a fraction ideal of $U^{-1}R$ and a straightforward computation shows that

$$\Big(U^{-1}\mathfrak{f}\Big)\Big(U^{-1}\mathfrak{g}\Big) \;=\; U^{-1}(\mathfrak{f}\,\mathfrak{g})$$

 In particular if $\mathfrak{f} \trianglelefteq_{\mathfrak{f}} R$ is invertible (over R) then $U^{-1}\mathfrak{f}$ is invertible (over $U^{-1}R$) and vice versa. Formally that is the equivalence

$$\mathfrak{f} \trianglelefteq_{\mathfrak{f}} R \text{ invertible} \quad\Longleftrightarrow\quad U^{-1}\mathfrak{f} \trianglelefteq_{\mathfrak{f}} U^{-1}R \text{ invertible}$$

Prob $(U^{-1}\mathfrak{f})\,(U^{-1}\mathfrak{g})$ is generated by elements of the form $(a/ub)(c/vd)$ where $a/b \in \mathfrak{f}$, $c/d \in \mathfrak{g}$ and u, $v \in U$. Now $uv \in U$ and $(a/ub)(c/vd) = (ac)/(uvbd)$ such that this is contained in $U^{-1}(\mathfrak{f}\,\mathfrak{g})$ again. This proves "$\subseteq$" conversely let $a/b \in \mathfrak{f}$, $c/d \in \mathfrak{g}$ and $u \in U$. Then $U^{-1}(\mathfrak{f}\,\mathfrak{g})$ is generated by elements of the form $(ac)/(ubd)$. And as $(ac)/(ubd) = (a/ub)(c/d)$ this is also contained in $(U^{-1}\mathfrak{f})\,(U^{-1}\mathfrak{g})$. This proves the converse inclusion "$\supseteq$" and hence the equality. And from this equality it is clear that $(U^{-1}\mathfrak{f})^{-1} = U^{-1}(\mathfrak{f}^{-1})$ for invertible fraction ideals (and hence the equivalence).

(2.159) Definition: (viz. 1111)
Let $(R,+,\cdot)$ be an integral domain and let us denote its quotient field by $F := \mathrm{QUOT}(R)$. Then R is said to be a **Dedekind domain** (shortly DKD) iff it satisfies one of the following equivalent statements

(a) every non-zero fraction ideal $0 \neq \mathfrak{f} \trianglelefteq_{\mathrm{f}} R$ is invertible (i.e. there is some fraction ideal $\mathfrak{g} \trianglelefteq_{\mathrm{f}} R$ such that $\mathfrak{f}\,\mathfrak{g} = R$).

(b) every non-zero (integral) ideal $0 \neq \mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ is invertible, (i.e. there is some fraction ideal $\mathfrak{g} \trianglelefteq_{\mathrm{f}} R$ such that $\mathfrak{a}\,\mathfrak{g} = R$).

(c) every (integral) ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ with $\mathfrak{a} \notin \{0, R\}$ allows a decomposition into finitely many prime ideals, i.e. $\exists\, \mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \mathrm{Spec}(R)$ such that $\mathfrak{a} = \mathfrak{p}_1 \ldots \mathfrak{p}_n$.

(d) R is a notherian, normal ring in which every non-zero prime ideal already is maximal, the latter being $\mathrm{Spec}(R) = \mathrm{Smax}(R) \cup \{0\}$.

(e) R is noetherian and for any non-zero prime ideal $0 \neq \mathfrak{p} \in \mathrm{Spec}(R)$ the localization $R_{\mathfrak{p}}$ is a discrete valuation ring (i.e. a local PID).

(2.160) Example:
In particular any PID $(R,+,\cdot)$ is a Dedekind domain - it is noetherian, as any ideal even has only one generator, it is normal (as it is an UFD by the fundamental theorem of arithmetic) and non-zero prime ideals are maximal (which can be seen using generators of the ideals).

(2.161) Theorem: (viz. 1116)
Let $(R,+,\cdot)$ be a Dedekind domain and $0 \neq \mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be a non-zero ideal of R. Then R already satisfies an extensive list of further properties, namely

(i) R is noetherian and every non-zero prime ideal of R already is maximal, the latter being

$$\mathrm{Spec}(R) \;=\; \mathrm{Smax}(R) \cup \{0\}$$

(ii) Any ideal $0 \neq \mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ admits a decomposition into finitely many (up to permutations) uniquely determined prime ideals, formally this is

$$\exists!\; \mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \mathrm{Spec}(R) \setminus \{0\} \quad \text{such that} \quad \mathfrak{a} = \mathfrak{p}_1 \ldots \mathfrak{p}_n$$

(iii) For any ideal $0 \neq \mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ the quotient ring $R/\mathfrak{a}$ is a principal ring (i.e. a ring in which any ideal is generated by a single element).

(iv) Any ideal of R can be generated by two elements already, we even get the slightly stronger property

$$\forall\, 0 \neq a \in \mathfrak{a} \;\; \exists\, b \in \mathfrak{a} \quad \text{such that} \quad \mathfrak{a} = aR + bR$$

(v) If R also is semilocal (i.e. R only has finitely many maximal ideals) then R already is a PID (i.e. every ideal is a principal ideal).

(vi) If $\mathfrak{m} \trianglelefteq_{\mathrm{i}} R$ is a maximal ideal of R and $1 \leq k \in \mathbb{N}$ then we obtain the following isomorphy of rings (where as usual $R_{\mathfrak{m}} = (R \setminus \mathfrak{m})^{-1}R$ and $\mathfrak{m}^k R_{\mathfrak{m}} = (R \setminus \mathfrak{m})^{-1}\mathfrak{m}^k \trianglelefteq_{\mathrm{i}} R_{\mathfrak{m}}$ denote the localization of R resp. the ideal corresponding to $\mathfrak{m}^k$)

$$R \Big/ \mathfrak{m}^k \;\cong_{\mathrm{r}}\; R_{\mathfrak{m}} \Big/ \mathfrak{m}^k R_{\mathfrak{m}} \;\; : \;\; a + \mathfrak{m}^k \mapsto \frac{a}{1} + \mathfrak{m}^k R_{\mathfrak{m}}$$

(2.162) Definition: (viz. 1114)
Let $(R, +, \cdot)$ be a Dedekind domain, $\mathfrak{m} \in \mathrm{Smax}(R)$ be a maximal ideal and $0 \neq \mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be a non-zero ideal of R. Then we define the **valuation** $\nu_{\mathfrak{m}}$ induced by $\mathfrak{m}$ on the set of ideals of R, by

$$\begin{aligned} \nu_{\mathfrak{m}} \;&:\; \mathrm{Ideal}(R) \to \mathbb{N} \\ &:\; \mathfrak{a} \mapsto \max\Big\{ k \in \mathbb{N} \mid \mathfrak{a} \subseteq \mathfrak{m}^k \Big\} \\ &:\; 0 \mapsto 0 \end{aligned}$$

And for any $a \in R$ we denote $\nu_{\mathfrak{m}}(a) := \nu_{\mathfrak{m}}(aR) \in \mathbb{N}$. Let now $\mathfrak{a}, \mathfrak{b} \trianglelefteq_{\mathrm{i}} R$ be arbitrary ideals of R. The we say that $\mathfrak{b}$ *divides* $\mathfrak{a}$, written as $\mathfrak{b} \mid \mathfrak{a}$, iff it satisfies one of the following equivalent properties:

$$\begin{aligned} \mathfrak{b} \mid \mathfrak{a} \quad &:\Longleftrightarrow \quad \exists\, \mathfrak{c} \trianglelefteq_{\mathrm{i}} R \;:\; \mathfrak{a} = \mathfrak{b}\mathfrak{c} \\ &\Longleftrightarrow \quad \mathfrak{a} \subseteq \mathfrak{b} \\ &\Longleftrightarrow \quad \forall\, \mathfrak{m} \in \mathrm{Smax}(R) \;:\; \nu_{\mathfrak{m}}(\mathfrak{b}) \leq \nu_{\mathfrak{m}}(\mathfrak{a}) \end{aligned}$$

(2.163) Proposition: (viz. 1114)
Let $(R, +, \cdot)$ be a Dedekind domain with quotient field $F := \mathrm{quot}(R)$. And let $\mathfrak{m} \trianglelefteq_{\mathrm{i}} R$ be any maximal (here this is non-zero prime) ideal of R. Then we obtain the following statements:

(i) Consider $\mathcal{M} = \{ \mathfrak{m}_1, \ldots, \mathfrak{m}_n \} \subseteq \mathrm{Smax}(R)$ a finite collection of maximal ideals and for each ideal some power $k(1), \ldots, k(n) \in \mathbb{N}$. Then for any $\mathfrak{m} \in \mathrm{Smax}(R)$ we obtain

$$\nu_{\mathfrak{m}}\left(\mathfrak{m}_1^{k(1)} \ldots \mathfrak{m}_n^{k(n)}\right) \;=\; \begin{cases} k(i) \text{ if } \mathfrak{m} = \mathfrak{m}_i \\ 0 \text{ if } \mathfrak{m} \notin \mathcal{M} \end{cases}$$

(ii) Consider any two non-zero ideals $0 \neq \mathfrak{a}, \mathfrak{b} \trianglelefteq_{\mathrm{i}} R$ then the multiplicity function $\nu_{\mathfrak{m}}$ acts additively under multiplication of ideals, that is

$$\nu_{\mathfrak{m}}(\mathfrak{a}\,\mathfrak{b}) \;=\; \nu_{\mathfrak{m}}(\mathfrak{a}) + \nu_{\mathfrak{m}}(\mathfrak{b})$$

(iii) Let $0 \neq \mathfrak{a}$, $\mathfrak{b} \trianglelefteq_{\mathrm{i}} R$ be any two non-zero ideals of R and decompose $\mathfrak{a} = \mathfrak{m}_1^{k(1)} \dots \mathfrak{m}_n^{k(n)}$ and $\mathfrak{b} = \mathfrak{m}_1^{l(1)} \dots \mathfrak{m}_n^{l(n)}$ with pairwise distinct maximal ideals $\mathfrak{m}_i \in \mathrm{Smax}(R)$ and $k(i), l(i) \in \mathbb{N}$ (note that this can always be established, as $k(i) = 0$ and $l(i) = 0$ is allowed). Then we get

$$\mathfrak{a} + \mathfrak{b} \;=\; \mathfrak{m}_1^{m(1)} \dots \mathfrak{m}_n^{m(n)} \quad \text{where} \quad m(i) := \min\{\, k(i), l(i) \,\}$$

(iv) Consider any non-zero ideal $0 \neq \mathfrak{a} \trianglelefteq_{\mathrm{i}} R$, as before we decompose $\mathfrak{a}$ into $\mathfrak{a} = \mathfrak{m}_1^{k(1)} \dots \mathfrak{m}_n^{k(n)}$ (with pairwise distinct $\mathfrak{m}_i \in \mathrm{Smax}(R)$ and $1 \leq k(i) \in \mathbb{N}$). Then we obtain *Chinese remainder theorem*:

$$R \Big/ \mathfrak{a} \;\cong_{\mathrm{r}}\; \bigoplus_{i=1}^{n} R \Big/ \mathfrak{m}_i^{k(i)} \;:\; b + \mathfrak{a} \mapsto \left(b + \mathfrak{m}_i^{k(i)} \right)$$

(v) Let $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be any ideal in R, then there is some ideal $\mathfrak{b} \trianglelefteq_{\mathrm{i}} R$ such that $\mathfrak{a} + \mathfrak{b} = R$ are coprime and $\mathfrak{a}\,\mathfrak{b}$ is principal (i.e. $\exists\, a \in R : \mathfrak{a}\,\mathfrak{b} = aR$).

2.13 Goldman Domains

This section should be skipped at a first exposition to the theory. Though it is not too far flung, it requires several concepts of ring extensions and Krull dimension that will be introduced in the chapters on module theory and ring extensions, only. Also the types of rings we are about to study here (Goldman domains, Hilbert rings and Jacobson rings) are rather restrictive and specific, it is rare to encounter these properties "in the field". However these rings contain the answer to several seemingly innocuous questions, that are surprisingly hard to answer. In our compilation of the matter we have seen several proofs that were either incomprehensible or severely flawed and probably both. All the more reason to present the theory in a comprehensible way with correct proofs. The key to achieving this lies in studying Hilbert and Jacobson rings simultaneously, in the end it turns out, that they really are the same thing.

(2.164) Definition: (viz. 1294)

(i) Let $(R,+,\cdot)$ be an integral domain and denote its quotient field by $E := \mathrm{QUOT}(R)$. Then R is said to be a **Goldman domain**, iff it satisfies one of the following three equivalent properties:

 (a) There is some $0 \neq u \in R$ such that the localisation R_u is a field.

 (b) There is some $0 \neq u \in R$ such that the quotient field of R is $E = R[1/u]$.

 (c) The quotient field E of R is finitely generated, as an R-algebra.

(ii) Let $(R,+,\cdot)$ be a commutative ring, then a prime ideal $\mathfrak{g} \trianglelefteq_{\mathrm{i}} R$ is said to be a **Goldmann ideal**, iff the quotient ring $R/\mathfrak{g}$ is a Goldman domain.

(iii) Let $(R,+,\cdot)$ be a commutative ring, then R is said to be a **Hilbert ring**, iff every Goldman ideal of R, already is a maximal ideal of R.

(2.165) Remark:

- By property (a) in a Goldman domain R, there is some $u \in R$ with $u \neq 0$, such that any element $x \in E$ of the quotient field is of the form $x = a/u^n$ for some $a \in R$ and some $n \in \mathbb{N}$. The element u can be taken to be the same for all elements $x \in E$.

- If $\mathfrak{g} \trianglelefteq_{\mathrm{i}} R$ is a Goldman ideal, then $R/\mathfrak{g}$ is an integral domain, as $\mathfrak{g}$ is prime. The second defining property means, that there is some $u \in R$ with $u \notin \mathfrak{g}$ such that the quotient field of $R/\mathfrak{g}$ is generated by the single element $1/(u+\mathfrak{g})$, formally

$$\mathrm{QUOT}\left(R\Big/\mathfrak{g}\right) \;=\; \left(R\Big/\mathfrak{g}\right)\left[\frac{1}{u+\mathfrak{g}}\right]$$

(2.166) Example:

- Any field $(F,+,\cdot)$ is a Goldman domain: Clearly localisation in 1 yields $F = F_1$ so F satisfies property (a) required for a Goldman domain. Also the ring of power series $F[\![t]\!]$ in one variable over a field is a Goldman domain. This is due to the fact that the quotient field of $F[\![t]\!]$ is the field of Laurent series $F[\![t]\!][t^{-1}]$, as we will see in (7.30.(v)). As this is the localisation of $F[\![t]\!]$ in t we have property (a) again.

- Likewise, if $p \in \mathbb{Z}$ is a prime number then the local ring $\mathbb{Z}_{(p)} := (\mathbb{Z} \setminus p\mathbb{Z})^{-1}\mathbb{Z}$ is a Goldman domain. This is due to the fact that we only need one more number to divide by, to build up the quotient field $\mathbb{Q} = \mathbb{Z}_{(p)}[1/p]$, so we have a Goldman domain by property (b) above.

- The ring of integers $\mathbb{Z}$ is a Hilbert ring, but not a Goldman domain. We will see this in greater generality in (2.169). A special case of this theorem is the following: If R is a PID, then R is a Hilbert ring if and only if R has infinitely many prime ideals. And R is a Goldman domain if and only if R has finitely many prime ideals only.

- The polynomial ring $R[t]$ will *never* be a Goldman domain. We will prove this in (2.167.(iii)) below, but the proof will already make use of (2.169), as well.

- If $(F, +, \cdot)$ is a field, then the polynomial ring $F[t]$ is a Jacobson ring and we will see in (2.171.(iv)) that this amounts to $F[t]$ being a Hilbert ring. And (2.170.(iv)) tells us that even $F[t_1, \ldots, t_n]$ is a Hilbert (equivalently a Jacobson) ring.

 Prob We will prove property (c) in the definition in (2.33) of Jacobson rings: If $\mathfrak{p} \trianglelefteq_{\mathrm{i}} F[t]$ is a prime ideal, we distinguish two cases: For $\mathfrak{p} = 0$ we get $\bigcap \{ \mathfrak{m} \in \operatorname{Smax}(F[t]) \mid \mathfrak{p} \subseteq \mathfrak{m} \} = \operatorname{JAC}(F[t])$ and by (2.7.(ii)) we know $\operatorname{JAC}(F[t]) = 0 = \mathfrak{p}$ by. And if $\mathfrak{p} \neq 0$, then $\mathfrak{p}$ already is maximal, as $F[t]$ is a PID and we have (2.79.(i)). Thus $\bigcap \{ \mathfrak{m} \in \operatorname{Smax}(F[t]) \mid \mathfrak{p} \subseteq \mathfrak{m} \} = \bigcap \{ \mathfrak{p} \} = \mathfrak{p}$.

(2.167) Proposition: (viz. 1295)

(i) Let $(R, +, \cdot)$ be a Goldman domain and denote its quotient field by $E := \operatorname{QUOT}(R)$. An itermediate ring S of $E : R$ (that is $S \subseteq E$ is an R-subalgebra of E) is a Goldman domain, as well.

(ii) If $(R, +, \cdot)$ is any commutative ring and $u \in R \setminus \operatorname{NIL}(R)$ is an element that is not a nilpotent of R, then there is a Goldman ideal $\mathfrak{g} \trianglelefteq_{\mathrm{i}} R$ such that $u \notin \mathfrak{g}$ and $(R/\mathfrak{g})_{u+\mathfrak{g}}$ is a field.

(iii) For any commutative ring $(R, +, \cdot)$, the polynomial ring $R[t]$ is *not* a Goldman domain. Consequentially, if $S : R$ is any ring extension in which R is an integral domain and $x \in S$ is any element, such that $R[x]$ is a Goldman domain, then $R[x] : R$ is algebraic.

(iv) If $(R, +, \cdot)$ is an integral domain with quotient field $E := \operatorname{QUOT}(R)$ and $u \in R$ is a non-zero element of R, then the following statements are equivalent

 (a) $E = R[1/u]$

 (b) R_u is a field

 (c) $u \in \bigcap \{ \mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \neq 0 \}$

 (d) $u \in \bigcap \{ \sqrt{\mathfrak{a}} \mid \mathfrak{a} \trianglelefteq_{\mathrm{i}} R, \mathfrak{a} \neq 0 \}$

(v) If $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ is an ideal of some commutative ring $(R, +, \cdot)$, then the radical of $\mathfrak{a}$ is the intersection of all Goldman ideals of R, that contain $\mathfrak{a}$, formally that is

$$\sqrt{\mathfrak{a}} = \bigcap \{ \mathfrak{g} \trianglelefteq_{\mathrm{i}} R \text{ Goldman ideal} \mid \mathfrak{a} \subseteq \mathfrak{g} \}$$

(vi) Let $(S,+,\cdot)$ be an integral domain and $R \subseteq S$ be a sub-ring, such that $S : R$ is algebraic. Then we get the implication (a) $\Longrightarrow$ (b) for the statements below. And if $S : R$ also is finitely generated, then we find the equivalence of

(a) R is a Goldman domain

(b) S is a Goldman domain

(2.168) Proposition: (viz. 816)

(i) Let $(R,+,\cdot)$ be a commutative ring and $\mathfrak{n} \trianglelefteq_{\mathrm{i}} R[t]$ be a maximal ideal of the polynomial ring. Suppose $\mathfrak{m} := \mathfrak{n} \cap R = \{\, a \in R \mid a\mathbf{1} \in \mathfrak{n} \,\}$ is a maximal ideal, too. Then there is a monic polynomial $f \in R[t]$ such that

(1) $\mathfrak{n} = \mathfrak{m}[t] + fR[t]$

(2) $f + \mathfrak{m}[t] \in R[t]/\mathfrak{m}[t]$ is a prime element

(ii) Let $(R,+,\cdot)$ be an integral domain and $E := \mathrm{QUOT}(R)$ be its quotient field. We denote the natural inclusion by $\iota : R[t] \hookrightarrow E[t]$, which is given to be $\iota(f) := \sum_k (f[k]/1)\, t^k$. Then we obtain a one-to-one correspondence between the prime ideals of $E[t]$ and the prime ideals $\mathfrak{p}$ of $R[t]$ that satisfy $\mathfrak{p} \cap R = 0$. And this correspondence is given to be

$$\begin{array}{rcl} \mathrm{Spec}\big(E[t]\big) & \longleftrightarrow & \big\{\, \mathfrak{p} \in \mathrm{Spec}\big(R[t]\big) \mid \mathfrak{p} \cap R = 0 \,\big\} \\ \mathfrak{u} & \mapsto & \{\, f \in R[t] \mid \iota(f) \in \mathfrak{u} \,\} \\ \left\{ \displaystyle\sum_{k=0}^{\infty} \frac{f[k]}{u} t^k \;\middle|\; f \in \mathfrak{p},\, u \neq 0 \right\} & \hookleftarrow & \mathfrak{p} \end{array}$$

(2.169) Theorem: (viz. 1297)
Let $(R,+,\cdot)$ be a noetherian integral domain. Then R is a Goldman domain if and only if R has only finitely many prime ideals. That is we have the equivalence

$$R \text{ Goldman domain} \iff \#\mathrm{Spec}(R) < \infty$$

Thereby the direction " $\Longleftarrow$ " is true for general integral domains R. And if R is a noetherian Goldman domain R, then R already is a field or a 1-dimensional domain, since we get

$$\mathrm{kdim}(R) \;\leq\; 1$$

Now suppose R is a noetherian integral domain of $\mathrm{kdim}(R) = 1$, that is $\mathrm{Spec}(R) = \mathrm{Smax}(R) \cup \{0\}$ where 0 is not a maximal ideal of R. Then the following four statements are equivalent

(a) $\mathrm{JAC}(R) = 0$

(b) $\mathrm{Spec}(R)$ is an infinite set

(c) R is a Hilbert ring

(d) R is *not* a Goldman domain

(2.170) Lemma: (viz. 1298)

(i) Let $(R,+,\cdot)$ be a Hilbert ring and consider any ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$. Then the quotient ring $R/\mathfrak{a}$ is a Hilbert ring, again.

(ii) Let $(R,+,\cdot)$ and $(S,+,\cdot)$ be commutative rings, such that S is a Hilbert ring. If $\varphi : S \twoheadrightarrow R$ is an epimorphism of rings, then R is a Hilbert ring, as well.

(iii) Let $(R,+,\cdot)$ be a Hilbert ring and A be a finitely generated R-algebra. Then (1) A is a Hilbert ring, as well and (2) if $\mathfrak{n} \in \operatorname{Smax}(A)$ is a maximal ideal, then $\mathfrak{m} := \mathfrak{n} \cap R \trianglelefteq_{\mathrm{i}} R$ is a maximal ideal of R, again. Finally, in this case, (3) $A/\mathfrak{n}$ is a finite field extension of $R/\mathfrak{m}$ [under the scalar multiplication $(a+\mathfrak{m})(f+\mathfrak{n}) := af+\mathfrak{n}$ where $a \in R$ and $f \in A$]

$$\left[A \Big/ \mathfrak{n} : R \Big/ \mathfrak{m} \right] \; < \; \infty$$

(iv) A special case of (iii) is the following: If $(R,+,\cdot)$ is a Hilbert ring, then $R[t_1,\ldots,t_n]$ is a Hilbert ring again. And if $\mathfrak{n}$ is a maximal ideal of $R[t_1,\ldots,t_n]$, then $\mathfrak{n} \cap R$ is a maximal ideal of R.

(2.171) Corollary: (viz. 1300)

(i) Let $(R,+,\cdot)$ be an integral domain, as we consider $R \subseteq R[t]$ to be a subset of the polynomial ring, we get $\mathfrak{u} \cap R = \{\, a \in R \mid a\mathbf{1} \in \mathfrak{u} \,\} \trianglelefteq_{\mathrm{i}} R$ for any ideal $\mathfrak{u} \trianglelefteq_{\mathrm{i}} R[t]$. And thereby the following four statements are equivalent

 (a) R is a Goldman domain

 (b) $0 \trianglelefteq_{\mathrm{i}} R$ is a Goldman ideal

 (c) $\bigcap \{\, \mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \neq 0 \,\} \neq 0$

 (d) there is some maximal ideal $\mathfrak{m} \trianglelefteq_{\mathrm{i}} R[t]$ such that $\mathfrak{m} \cap R = 0$

(ii) Let $(F,+,\cdot)$ be any commutative ring, then the following three properties are equivalent

 (a) F is a field

 (b) F is a Goldman domain satisfying $\textsc{jac}(F) = 0$

 (b) F is a Goldman domain and Hilbert ring

(iii) Let $(R,+,\cdot)$ be a commutative ring and $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ be a prime ideal of R. Then $\mathfrak{p}$ has been defined to be a Goldman ideal, iff (a). And this property (a) is equivalent to two other properties (b), (c) that are given to be

 (a) $R/\mathfrak{p}$ is a Goldman domain

 (b) there is some $u \in \bigcap \{\, \mathfrak{q} \in \operatorname{Spec}(R) \mid \mathfrak{p} \subset \mathfrak{q} \,\} \setminus \mathfrak{p}$

 (c) there is some maximal ideal $\mathfrak{m} \trianglelefteq_{\mathrm{i}} R[t]$ such that $\mathfrak{p} = \mathfrak{m} \cap R$

(iv) Let $(R,+,\cdot)$ be any commutative ring, then the following four properties are equivalent

(a) R is a Hilbert ring

(b) R is a Jacobson ring

(c) If $\mathfrak{m} \in \mathrm{Smax}(R[t])$ then $\mathfrak{m} \cap R \trianglelefteq_{\mathrm{i}} R$ is a maximal ideal again

(d) *Zariski's Lemma:* If A is a finitely generated R algebra, such that A is a field, then A already is finitely generated, as an R-module.

NOTA We have found 3 equivalent properties for Goldman domains in (2.164.(i)) and another 3 in (i) above. A Jacobson ring has been defined in (2.33) by 6 equivalent properties. Altogether the above list (iv) thereby boasts 14 different equivalences!

(2.172) Lemma: (viz. 1303)
Let $(R,+,\cdot)$ be a Jacobson ring, as defined in (2.33) - note that by (2.171.(iv)) this is equivalent to R being a Hilbert ring. Then the Jacobson property has the following hereditary properties:

(i) For any ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ the quotient ring $R/\mathfrak{a}$ is jacobson.

(ii) If $\varphi : R \twoheadrightarrow S$ is an epimorphism of rings onto another ring $(S,+,\cdot)$, then the image S is jacobson.

(iii) If $S : R$ is an integral ring extension, where R and S are arbitrary commutative rings, then R is jacobson, if and only if S is jacobson.

(iv) For any $u \in R$ the localisation R_u is a Jacobson ring again and the one-to-one correspondence of prime ideals of R_u extends to maximal ideals, that is we get

$$\begin{array}{rcl} \mathrm{Smax}\big(R_u\big) & \longleftrightarrow & \{\, \mathfrak{m} \in \mathrm{Smax}(R) \mid u \notin \mathfrak{m} \,\} \\ \mathfrak{n} & \mapsto & \mathfrak{n} \cap R \\ \mathfrak{m}\, R_u & \hookleftarrow & \mathfrak{m} \end{array}$$

NOTA If $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ is a prime ideal, then the localisation $R_{\mathfrak{p}}$ need *not* be jacobson. If it was, we had $\mathrm{NIL}(R_{\mathfrak{p}}) = \mathrm{JAC}(R_{\mathfrak{p}}) = \mathfrak{p}R_{\mathfrak{p}}$ as $R_{\mathfrak{p}}$ is a local ring. But this implies $\mathfrak{p} = 0$ already.

Chapter 3

Modules

3.1 Defining Modules

The notion of a module is *the* cornerstone of algebra - it is sufficiently general to cover countless different situations, of all fields of mathematics and specific enough, as to produce a vast amount of properties to exploit. Because of its importance we have chosen to give a very precise definition of what a module is exactly: For the time being we use the binary operation $\diamond$ to denote the scalar multiplication in order to be able to write down the properties of a module in great detail. However we will soon follow the customary simplification to just write ax instead of $a \diamond x$, as the properties of a module will guarantee that this can be done safely.

(3.1) Definition:
Let $(R, +, \cdot)$ be a ring, then the triple $(M, +, \diamond)$ is said to be an R**-module**, iff $M \neq \emptyset$ is a non-empty set and $+$ resp. $\diamond$ are binary operations of the form $+ : M \times M \to M : (x, y) \mapsto x + y$ and $\diamond : R \times M \to M : (a, x) \mapsto a \diamond x = ax$, that satisfy the following properties

(G) $(M, +)$ is a commutative group, that is the addition $+$ is *associative* and *commutative*, admits a neutral element (called the *zero-element*, which will be denoted by 0) and every element of M has an additive inverse. Formally

$$\begin{aligned} \forall\, x, y, z \in M &: x + (y + z) = (x + y) + z \\ \forall\, x, y \in M &: x + y = y + x \\ \exists\, 0 \in M\, \forall\, x \in M &: x + 0 = x \\ \forall\, x \in M\, \exists\, \overline{x} \in M &: x + \overline{x} = 0 \end{aligned}$$

(M) The *addition* $+$ and *scalar multiplication* $\diamond$ on M satisfy the following compatibility conditions regarding the operations of R

$$\begin{aligned} \forall\, a \in R\, \forall\, x, y \in M &: a \diamond (x + y) = (a \diamond x) + (a \diamond y) \\ \forall\, a, b \in R\, \forall\, x \in M &: (a + b) \diamond x = (a \diamond x) + (b \diamond x) \\ \forall\, a, b \in R\, \forall\, x \in M &: (a \cdot b) \diamond x = a \diamond (b \diamond x) \\ \forall\, x \in M &: 1 \diamond x = x \end{aligned}$$

(3.2) Remark:

- The notations in the definition above deserve some special attention. First note that - as always with binary operations - we wrote $x+y$ instead of $+(x,y)$. Likewise $a \diamond x$ instead of $\diamond(a,x)$ and of course $a+b$ instead of $+(a,b)$, $a \cdot b$ instead of $\cdot(a,b)$ (as we already did with rings).

- Recall that for a ring $(R,+,\cdot)$ the operation $+$ has been called *addition* and $\cdot$ has been called *multiplication* of R. In analogy, if $(M,+,\diamond)$ is an R-module, then $+$ is said to be the *addition* of M and $\diamond$ is called the *scalar multiplication* of M.

- Next note that we have used two different binary operations $+$, namely $+ : R \times R \to R$ of $(R,+,\cdot)$ and $+ : M \times M \to M$ of $(M,+,\diamond)$. At first it may be misleading to denote two different functions by the same symbol, but you will soon become used to it and appreciate the simplicity of this notation. It will not lead to ambiguities, as the neighbouring elements (a and b for $a+b$ in R, resp. x and y for $x+y$ in M) determine which of the two functions is to be applied. As an exercise it might be useful to rewrite the defining properties (M) using $+_R$ for $+$ in R and $+_M$ for $+$ in M. As an example let us reformulate the first two properties in this way

$$\begin{aligned} \forall\, a \in R\ \forall\, x,y \in M \quad a \diamond (x +_M y) &= (a \diamond x) +_M (a \diamond y) \\ \forall\, a,b \in R\ \forall\, x \in M \quad (a +_R b) \diamond x &= (a \diamond x) +_M (b \diamond x) \end{aligned}$$

- Note that the properties (G) of R-modules truly express that $(M,+)$ is a commutative group. In particular we employ the usual notational conventions for groups. E.g. we may omit the bracketing in sums due to the associativity of the addition $+$ of M

$$x+y+z := (x+y)+z$$

$$\sum_{i=1}^{n} x_i := \Big((x_1+x_2)+\ldots\Big)+x_n$$

 And as always the *neutral element* $0 \in M$ is uniquely determined again (if 0 and $0'$ are neutral elements, then $0' = 0+0' = 0'+0 = 0$). Likewise given $x \in M$ there is a uniquely determined $\overline{x} \in M$ such that $x+\overline{x} = 0$ and this is said to be the *negative* element of x, denoted by $-x := \overline{x}$ (if p and q are negative elements of x then $p = p+0 = p+(x+q) = q+(x+p) = q+0 = q$).

- Let $(R,+,\cdot)$ be any ring (with unit element 1) and M be an R-module, then we note some immediate consequences of the axioms above. Let $x \in M$ and recall that $-x$ denotes the negative of x, then

$$\begin{aligned} 0 \diamond x &= 0 \\ (-1) \diamond x &= -x \end{aligned}$$

 Prob as $0 = 0+0$ in R we get $0 \diamond x = (0+0) \diamond x = (0 \diamond x) + (0 \diamond x)$ from (M). And substracting $0 \diamond x$ once from this equality we find $0 = 0 \diamond x$. This may now be used to see $0 = 0 \diamond x = (1+(-1)) \diamond x = (1 \diamond x) + ((-1) \diamond x)$. Substracting $x = 1 \diamond x$ we find $-x = (-1) \diamond x$.

- We have already simplified the notations for modules rigorously. However it is still useful to introduce some further conventions. Recall that for rings $(R,+,\cdot)$ we wrote ab instead of $a\cdot b$. And we wrote $a-b$ instead of $a+(-b)$ and $ab+c$ instead of $(a\cdot b)+c$. The same is true for the addition in the module M: We will write $x-y$ instead of $x+(-y)$. Likewise we write ax instead of $a\diamond x$ and declare that the scalar multiplication $\diamond$ is of higher priority that the addition $+$. E.g.

 $$ax+y \;:=\; (a\diamond x)+y$$

 Note that it is unambiguously to write abx instead of the original terms $(a\cdot b)\diamond x = a\diamond(b\diamond x)$, as this equality has been one of the axioms for R-modules. Thus we may also omit the brackets in mixed terms with multiplication and scalar multiplication. These conventions contribute to the readability of the expressions, as you can surely see already.

- In contrast to rings (where we faithfully wrote $(R,+,\cdot)$ on every first occurrance of the ring) we will omit the operations $+$ and $\diamond$ when referring to the R-module $(M,+,\diamond)$. That is we will say "let M be an R-module" and think of $(M,+,\diamond)$ instead of M.

- What we defined here is also called a **left R-module**, this is to say that in the scalar multiplication $\diamond : R\times M\to M$ the ring R acts from the left. One might be tempted to regard right R-modules as well, i.e. structures $(M,+,\curvearrowleft)$ in which the ring R acts from the right $\curvearrowleft : M\times R\to M : (x,a)\mapsto x\curvearrowleft a$ that satisfy the analogous properites $(x+y)\curvearrowleft a = (x\curvearrowleft a)+(y\curvearrowleft a)$, $x\curvearrowleft(a+b) = (x\curvearrowleft a)+(x\curvearrowleft b)$, $x\curvearrowleft(a\cdot b) = (x\curvearrowleft a)\curvearrowleft b$ and $x\curvearrowleft 1 = x$. However this would only yield an entirely analogous theory: Recall the construction of the *opposite ring* $(R,+,\cdot)^{\mathrm{op}}$ in section 1.4. If $(M,+,\diamond)$ is a (left) R-module, then we obtain a right R^{op}-module $(M,+,\diamond)^{\mathrm{op}}$ by taking M as a set and $+$ as an addition again, but using a scalar multiplication that reverses the order of elements. That is we obtain a right R^{op}-module by

 $$(M,+,\diamond)^{\mathrm{op}} \;:=\; (M,+,\curvearrowleft) \text{ where } x\curvearrowleft a := a\diamond x$$

- The theory of R-modules is particularly simple in the case that the base ring R is a field. As this case historically has been studied first there is some special nomenclature: Suppose that V is an F-module, where $(F,+,\cdot)$ is a field. Then we will use the following notions

set theory	linear algebra
$(F,+,\cdot)$	base field
$(V,+,\diamond)$	vector space
elements of F	scalars
elements of V	vectors

(3.3) Example:

- Consider any commutative group $(G,+)$, then G becomes a $\mathbb{Z}$-module under the following scalar multiplication $\diamond : \mathbb{Z} \times G \to G$ [take a look at (1.29) for a proof]

$$k \diamond x \;:=\; \begin{cases} \sum_{i=1}^{k} x \text{ for } k > 0 \\ 0 \text{ for } k = 0 \\ \sum_{i=1}^{-k} (-x) \text{ for } k < 0 \end{cases}$$

- Let $(R,+,\cdot)$ be any ring and $\mathfrak{a} \;\leq_{\mathfrak{m}}\; R$ be a left-ideal of R (note that in particular $\mathfrak{a} = R$ is allowed). Then $\mathfrak{a}$ is an R module under the operations inherited from R, that is

$$\begin{aligned} + \;:\; \mathfrak{a} \times \mathfrak{a} \to \mathfrak{a} \;&:\; (x,y) \mapsto x+y \\ \diamond \;:\; R \times \mathfrak{a} \to \mathfrak{a} \;&:\; (a,x) \mapsto ax \end{aligned}$$

 That is: Although we started with quite a lot of axioms for R-modules, examples are abundant - the theory of modules encompasses the theory of rings! And the proofs are full of examples how module theory can be put to good use in ring theory (e.g. the lemma of Nakayama).

- Consider any (not necessarily commutative) ring $(S,+,\cdot)$ and suppose $R \;\leq_{\mathrm{r}}\; S$ is a sub-ring of S. If now M is an S-module, then M becomes an R-module under the operations inherited from S

$$\begin{aligned} + \;:\; M \times M \to M \;&:\; (x,y) \mapsto x+y \\ \diamond \;:\; R \times M \to M \;&:\; (a,x) \mapsto ax \end{aligned}$$

- Let $(R,+,\cdot)$ and $(S,+,\cdot)$ be any two (not necessarily commutative) rings and consider a ring-homomorphism $\varphi : R \to S$. If now M is an S-module, then M also becomes an R-module under

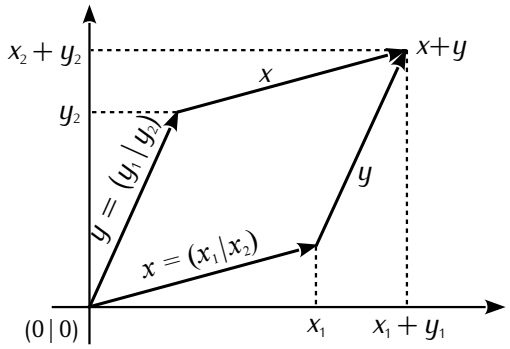
$$\begin{aligned} + \;:\; M \times M \to M \;&:\; (x,y) \mapsto x+y \\ \diamond \;:\; R \times M \to M \;&:\; (a,x) \mapsto \varphi(a)x \end{aligned}$$

- Consider an arbitrary (not necessarily commutative) ring $(R,+,\cdot)$. Then R^n becomes an R-module (for any $1 \leq n \in \mathbb{N}$) under the point-wise operations $+ : R^n \times R^n \to R^n$ and $\diamond : R \times R^n \to R^n$

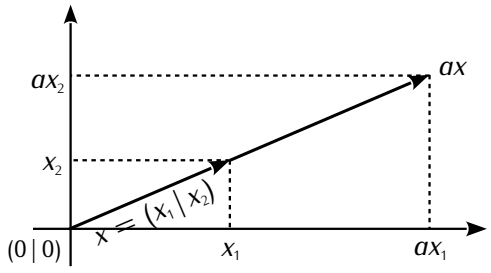
$$\begin{aligned} (x_1,\ldots,x_n) + (y_1,\ldots,y_n) \;&:=\; (x_1+y_1,\ldots,x_n+y_n) \\ a \diamond (x_1,\ldots,x_n) \;&:=\; (a \cdot x_1,\ldots,a \cdot x_n) \end{aligned}$$

 Note that the operations $+$ and $\cdot$ on the right hand side are those of the ring R, whereas the operations $+$ and $\diamond$ are thereby defined for the module R^n. Further note that in the case $n = 1$ we get $R^n = R$ and the addition $+$ on R^1 by definition coincides with the addition $+$ on R. This is precisely the reason why we did not need to distinguish between $+_R$ and $+_M$ - in case of doubt it doesn't matter, it's just the same.

(3.4) Remark:
The example R^n is the most basic and most important case of a module: It is the prototype of any free, finitely generated module, which is the best class of modules around. But it also is the first module that has been studied: In the case of the reals $R = \mathbb{R}$ the vector-spaces $\mathbb{R}^2$ and $\mathbb{R}^3$ are the domains of plane resp. of spatial geometry. And the addition of vectors in $\mathbb{R}^3$ is the way to describe the addition of velocities or forces in physics. It is here that we gain an intuition of what the addition and scalar multiplication of vectors is about:
First of a an n-tuple $x = (x_1, \ldots, x_n) \in R^n$ designates a point in space. But likewise we can think of x as an arrow pointing from the origin $0 \in R^n$ to x. From a mathematical point of view there is *no* distinction between points and arrows, as both are n-tuples. And there is good reason not to introduce any artificial distinction:
So this is what the addition $x + y$ of two n-tuples x, $y \in R^n$ does: It starts at point x and attaches the arrow y to it. Then the shifted arrow y ends at the point $x + y$. But you can also look at it in the following way: Start with the arrow x and attach arrow y (so that y starts, where x ends). Then the arrow $x + y$ points from 0 straight to the end of the shifted arrow y. That is $x + y$ is the diagonal in the parallelogram with the sides x and y:



It is a remarkable fact that nature can be described in these simple terms, but for marvellous reasons the addition of forces (amongst many other things) is precisely the point-wise addition of tuples in $\mathbb{R}^3$.
The scalar multiplication of R^n is understood best, if we think of an n-tuple x to be an arrow from 0 to x again. Then ax is just the arrow x stretched by the factor $a \in R$. (In case of $a < 1$ this is a reduction of length and in case $a < 0$ the arrow ax also points in the opposite direction).



(3.5) Definition:
Let $(R,+,\cdot)$ be a ring, then the quadrupel $(A,+,\cdot,\diamond)$ is said to be an R**-semi-algebra**, iff $A \neq \emptyset$ is a non-empty set and $+$, $\cdot$ resp. $\diamond$ are binary opertations of the form $+ : A \times A \to A$, $\cdot : A \times A \to A$ and $\diamond : R \times A \to A$ that satisfy the following properties

(R) $(A,+,\cdot)$ is a semi-ring, that is the addition $+$ is *associative* and *commutative*, admits a neutral element (called *zero-element*, denoted by 0), every element of A has an additive inverse, the multiplication $\cdot$ is *associative* and satisfies the *distributivity laws*. Formally

$$\begin{aligned}
\forall f,g,h \in A &: f+(g+h) = (f+g)+h \\
\forall f,g \in A &: f+g = g+f \\
\exists 0 \in A\, \forall f \in A &: f+0 = f \\
\forall f \in A\, \exists \overline{f} \in A &: f+\overline{f} = 0 \\
\forall f,g,h \in A &: f\cdot(g\cdot h) = (f\cdot g)\cdot h \\
\forall f,g,h \in A &: f\cdot(g+h) = (f\cdot g)+(f\cdot h) \\
\forall f,g,h \in A &: (f+g)\cdot h = (f\cdot h)+(g\cdot h)
\end{aligned}$$

(M) $(A,+,\diamond)$ is an R-module, that is the *addition* $+$ and *scalar multiplication* $\diamond$ of A satisfy the following compatibility conditions

$$\begin{aligned}
\forall a \in R\, \forall f,g \in A &: a\diamond(f+g) = (a\diamond f)+(a\diamond g) \\
\forall a,b \in R\, \forall f \in A &: (a+b)\diamond f = (a\diamond f)+(b\diamond f) \\
\forall a,b \in R\, \forall f \in A &: (a\cdot b)\diamond f = a\diamond(b\diamond f) \\
\forall f \in A &: 1\diamond f = f
\end{aligned}$$

(A) The *multiplication* $\cdot$ and *scalar multiplication* $\diamond$ of A are compatible in the following sense (note that this is some kind of associativity)

$$\forall a \in R\, \forall f,g \in A : (a\diamond f)\cdot g = a\diamond(f\cdot g) = f\cdot(a\diamond g)$$

If now $(A,+,\cdot,\diamond)$ is an R-algebra, then we transfer most of the notions of ring theory to the case of algebras, by refering to the semi-ring $(A,+,\cdot)$. To be precise introduce the following notions

$(A,+,\cdot,\diamond)$ is called		$(A,+,\cdot)$ is a(n)
R-algebra	$:\Longleftrightarrow$	ring
commutative	$:\Longleftrightarrow$	commutative
integral	$:\Longleftrightarrow$	integral domain
division algebra	$:\Longleftrightarrow$	skew-field
noetherian	$:\Longleftrightarrow$	commutative, noetherian ring
artinian	$:\Longleftrightarrow$	commutative, artinian ring
local	$:\Longleftrightarrow$	commutative, local ring
semi-local	$:\Longleftrightarrow$	commutative, semi-local ring

(3.6) Remark:

- By definition any R-semi-algebra $(A, +, \cdot, \diamond)$ has a (uniquely determined) neutral element of addition, denoted by 0 (that is $f + 0 = f$ for any $f \in A$). To be an R-algebra by definition means that the multiplication also admits a neutral element. That is there is some $1 \in A$ such that for any $f \in A$ we get $f \cdot 1 = f = 1 \cdot f$. And due to the associativity of $\cdot$ this *unit element* 1 is uniquely determined again.

- If $(A, +, \cdot, \diamond)$ is an R-algebra, then by definition $(A, +, \cdot)$ is a semi-ring and $(A, +, \diamond)$ is an R-module. In particular A inherits all the properties of these objects and we also pick up all notational conventions introduced for these objects. That is we write 0 for the zero-element and 1 for the unit element (supposed A is an R-algebra). Likewise we write $-f$ for the additive inverse of f (that is $f + (-f) = 0$ and f^{-1} for the multiplicative inverse of f (that is $f \cdot f^{-1} = 1 = f^{-1} \cdot f$), supposed such an element exists. In case you are not familiar with these conventions we recommend having a look at section 1.3.

- If A is a *commutative* R-semi-algebra, then condition (A) boils down to $(a \diamond f) \cdot g = a \diamond (f \cdot g)$ for any $a \in R$ and $f, g \in A$. Because if this property is satisfied then we already get $(a \diamond f) \cdot g = f \cdot (a \diamond g)$ from the commutativity $f \cdot (a \diamond g) = (a \diamond g) \cdot f = a \diamond (g \cdot f) = a \diamond (f \cdot g) = (a \diamond f) \cdot g$.

- If A is an R-algebra, i.e. an R-semi-algebra containing a unit element 1, then due to property (A) the scalar multiplication $\diamond$ can be expressed in terms of the ordinary multiplication of A with elements of the form $a \diamond 1$. To be precise, let $a \in R$ and $f \in A$, then we clearly obtain

$$(a \diamond 1) \cdot f \quad = \quad a \diamond f$$

- If $(R, +, \cdot)$ is an arbitrary (i.e. not necessarily commutative) ring and A is an R algebra with unit element 1_A then the elements $a1_A = a \diamond 1_A$ commute with any element $f \in A$. That is

$$\{\, a1_A \mid a \in R \,\} \quad \subseteq \quad \text{CEN}(A)$$

 This is due to property (A) of R-semi-algebras, as for any $a \in R$ and $f \in A$ we may compute $(a \diamond 1_A) \cdot f = a \diamond (1_A \cdot f) = a \diamond (f \cdot 1_A) = f \cdot (a \diamond 1_A)$.

- Note that property (A) in the definition of R-semi-algebras enables us to not only omit the multiplicative symbol $\cdot$ and scalar multiplication $\diamond$ but also the bracketing. Whenever we have a term of the form afg then we may use either bracketing $(af)g = a(fg)$ due to (A).

- Even if $a1_A = b1_A \in A$ we may *not* conclude $a = b \in R$. As a counterexample consider $A = \mathbb{Z}_4$ which is an algebra over $R = \mathbb{Z}$. Then we have $1_A = 1 + 4\mathbb{Z}$ and $21_A = 61_A$. Later on we will give a name to this property: In a *torsion-free* R-algebra we may conclude $a = b$ from $a1_A = b1_A$.

- Let $(R, +, \cdot)$ be a commutative ring and A be an R-semi-algebra, then we can embed A into an R-algebra A' canonically: As a set take $A' := R \times A$ and define the following operations on A'

$$\begin{aligned} (a, f) + (b, g) &:= (a + b, f + g) \\ (a, f) \cdot (b, g) &:= (ab, fg + ag + bf) \end{aligned}$$

$$a \diamond (b,g) \quad := \quad (ab, ag)$$

Then $(A', +, \cdot, \diamond)$ truly becomes an R-algebra (the verification of this is left to the interested reader) with zero element $(0,0)$ and unit element $(1,0)$. And of course we get a canonical embedding (i.e. an injective homomorphism of R-algebras), by virtue of

$$A \hookrightarrow A' \; : \; f \mapsto (0, f)$$

(3.7) Example:

- Let $(R, +, \cdot)$ be a commutative ring then, R becomes an R-module (even an R-algebra) canonically under its addition $+$ as an addition of vectors and its multiplication $\cdot$ as both, its multiplication and scalar-multiplication. I.e. if we let $A := R$, then R becomes an R-algebra $(A, +, \cdot, \diamond)$, under the operations

$$\begin{aligned} + \; : \; A \times A \to A \quad &: \quad (f,g) \mapsto f + g \\ \cdot \; : \; A \times A \to A \quad &: \quad (f,g) \mapsto fg \\ \diamond \; : \; R \times A \to A \quad &: \quad (a,f) \mapsto af \end{aligned}$$

 In the following - whenever we say that we regard some ring $(R, +, \cdot)$ as an R-module - we will refer to this construction. And in this case any subset $\mathfrak{a} \subseteq R$ is an ideal of R if and only if i t is an R-sub-module

$$\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R \quad \Longleftrightarrow \quad \mathfrak{a} \leq_{\mathfrak{m}} R$$

- Let $(R, +, \cdot)$ be a commutative ring again and $I \neq \emptyset$ be any non-empty set, then we take to be the set $A := \mathcal{F}(I, R)$ of functions from I to R. Note that this includes the case $A = R^n$ by taking $I := 1 \ldots n$. Then A becomes an R-algebra $(A, +, \cdot, \diamond)$, under the point-wise operations

$$\begin{aligned} + \; : \; A \times A \to A \quad &: \quad (f,g) \mapsto (i \mapsto f(i) + g(i)) \\ \cdot \; : \; A \times A \to A \quad &: \quad (f,g) \mapsto (i \mapsto f(i) \cdot g(i)) \\ \diamond \; : \; R \times A \to A \quad &: \quad (a,f) \mapsto (i \mapsto af(i)) \end{aligned}$$

- Likewise let $(R, +, \cdot)$ be a commutative ring and $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$ be an ideal of R. Then we may consider the quotient ring $A := R/\mathfrak{a}$ as an R-algebra $(A, +, \cdot, \diamond)$, under the following operations

$$\begin{aligned} + \; : \; A \times A \to A \quad &: \quad (b + \mathfrak{a}, c + \mathfrak{a}) \mapsto (b + c) + \mathfrak{a} \\ \cdot \; : \; A \times A \to A \quad &: \quad (b + \mathfrak{a}, c + \mathfrak{a}) \mapsto (bc) + \mathfrak{a} \\ \diamond \; : \; R \times A \to A \quad &: \quad (a, b + \mathfrak{a}) \mapsto (ab) + \mathfrak{a} \end{aligned}$$

- This is a special case of the following general concept: Consider any two commutative rings $(R, +, \cdot)$ and $(A, +, \cdot)$ and regard an arbitrary ring-homomorphism $\varphi : R \to A$. Then A can be considered to be an R-algebra under its own addition $+$ and its own multiplication $\cdot$ as multiplication and the scalar multiplication is multiplication in A with the imported elements $\varphi(a)$. That is A becomes an R-algebra under the operations

$$
\begin{aligned}
+ \;:\; A \times A \to A \quad &:\quad (f,g) \mapsto f+g \\
\cdot \;:\; A \times A \to A \quad &:\quad (f,g) \mapsto fg \\
\diamond \;:\; R \times A \to A \quad &:\quad (a,f) \mapsto \varphi(a)f
\end{aligned}
$$

- Generally: If $(S,+,\cdot)$ is a semi-ring, then $(S,+)$ can not only turned into an $\mathbb{Z}$-module, but S even becomes a $\mathbb{Z}$-semi-algebra under its own addition and multiplication and $\mathbb{Z} \times S \to S : (a,x) := ax$ as a scalar multiplication. Recall that in (3.3) we have defined the scalar multiplication ax to be $ax := 0$ for $a = 0$, $ax := x + x + \cdots + x$ (a-times) for $a > 0$ and $ax := (-a)(-x)$ for $a < 0$. A proof of this statement is provided in the proof of (1.29).

- The most general case of the above is the following: Let $(R,+,\cdot)$ be any (that is even a non-commutative) ring. Then R still is an R-module under the above operations. But R no longer needs to be R-algebra. Likewise consider a second ring $(S,+,\cdot)$ and a ring-homomorphism $\varphi : R \to S$. Then S is an R-module under the above operations.

 $$
 \begin{aligned}
 + \;:\; S \times S \to S \quad &:\quad (x,y) \mapsto x+y \\
 \diamond \;:\; R \times S \to S \quad &:\quad (a,x) \mapsto \varphi(a)y
 \end{aligned}
 $$

 Again S, need not be an R-algebra, in general. However S becomes an R-algebra (under its own multiplication), if the image of R under φ is contained in the center of S, that is if

 $$\varphi(R) \quad \subseteq \quad \text{CEN}(S) \;:=\; \{\, x \in S \mid \forall\, y \in S : xy = yx \,\}$$

- An example of the above situation will be the ring of $n \times n$ matrices over a commutative ring $(R,+,\cdot)$. Recall the construction of matrices given in section 1.4 (for more details confer to section 4.1) and let $S := \text{mat}_n(R)$. Then we obtain a homomorphism of rings by letting

 $$\varphi \;:\; R \to S \;:\; a \mapsto \begin{pmatrix} a & & 0 \\ & \ddots & \\ 0 & & a \end{pmatrix}$$

 And as R is commutative it is clear, that $\varphi(R) \subseteq \text{CEN}(S)$ (in fact it even is true that $\varphi(R) = \text{CEN}(S)$) and hence S becomes a well-defined R-algebra (under the usual multiplication and addition of matrices). Of course this multiplication is just the same, as the point-wise multiplication by a.

(3.8) Definition:
Let $(R,+,\cdot)$ be a ring and M be an R-module. Then a subset $P \subseteq M$ is said to be an **R-sub-module** of M, iff it satisfies the following three properties

(1) $0 \in P$

(2) $x, y \in P \implies x + y \in P$

(3) $a \in R,\, x \in P \implies ax \in P$

And in this case we will write $P \leq_{\mathfrak{m}} M$. Likewise if A is a R-semi-algebra and $P \subseteq A$ is a subset, then P is said to be an R-**sub-semi-algebra**, iff it is both, a sub-module and sub-semi-ring of A Formally iff

(M) $P \leq_{\mathfrak{m}} A$

(4) $f, g \in P \implies fg \in P$

And in this case we will write $P \leq_{\mathfrak{b}} A$. In this case P is said to be an **unital** R-**sub-semi-algbra** iff P contains a unit element for itself, that is iff P satisfies the properties

(B) $P \leq_{\mathfrak{b}} A$

(U) $\exists\, e \in P$ such that $\forall\, f \in P$ we have $ef = f = fe$

If the unit element $e \in P$ is just the unit element $1 \in A$ (that is, in case P is both, a sub-module and sub-ring of A) then P is said to be an R-**subalgebra** of A, formally that is iff P satisfies

(B) $P \leq_{\mathfrak{b}} A$

(5) $1 \in P$

And in this case we will write $P \leq_{\mathfrak{a}} A$. Let now A be an R-semi-algebra again. Then a subset $\mathfrak{a} \subseteq A$ is said to be an R-**algebra-ideal** of A. iff it is both, an ideal and a sub-module of A, formally iff it satisfies

(M) $\mathfrak{a} \leq_{\mathfrak{m}} A$

(I) $f \in \mathfrak{a}, g \in A \implies fg \in \mathfrak{a}$ and $gf \in \mathfrak{a}$

And in this case we write $\mathfrak{a} \trianglelefteq_{\mathfrak{a}} A$. Having defined all these notions the set of all sub-modules of an R-module M is denoted by $\mathrm{Subm}(M)$. Likewise $\mathrm{Subb}(A)$ denotes the set of all R-sub-semi-algebras, $\mathrm{aIdeal}(A)$ denotes the set of all algebra-ideals of a semi-algebra A. And finally the set of all R-subalgebras of an R-algebra A id denoted by $\mathrm{Suba}(A)$. Formally we define

$$\begin{aligned}
\mathrm{Subm}(M) &:= \{\, P \subseteq M \mid P \leq_{\mathfrak{m}} M \,\} \\
\mathrm{Subb}(A) &:= \{\, P \subseteq A \mid P \leq_{\mathfrak{b}} A \,\} \\
\mathrm{Suba}(A) &:= \{\, P \subseteq A \mid P \leq_{\mathfrak{a}} A \,\} \\
\mathrm{aIdeal}(A) &:= \{\, \mathfrak{a} \subseteq A \mid P \leq_{\mathfrak{b}} A \,\}
\end{aligned}$$

(3.9) Remark:

- If $P \leq_{\mathfrak{m}} M$ is a sub-module (of the R-module M, where $(R, +, \cdot)$ is an arbitrary ring), then $P \leq_{\mathfrak{g}} M$ already is a *subgroup* of $(M, +)$, too. That is $0 \in P$ and for any $x, y \in P$ we get $-x \in P$ and $x + y \in P$. Thereby $-x \in P$ follows from (3) by regarding $a := -1$, as in this case we get $-x = (-1) \diamond x \in P$ already.

- Likewise if A is an R-algebra (over an arbitrary ring $(R, +, \cdot)$), then we only need to check properties (1), (2), (4) and (5), as (3) follows from (4): Given $f \in R$ and $a \in A$ we get $af = (a1_A) \diamond f \in P$.

- Let A be an R-semi-algebra over the ring $(R, +, \cdot)$, then any sub-semi-algebra of A already is a a sub-semi-ring of A, formally

$$P \leq_{\mathrm{b}} A \quad \Longrightarrow \quad P \leq_{\mathrm{s}} A$$

 Prob Properties (1), (2) and (4) of sub-semi-algebras and sub-semi-rings coincide. It only remains to check property (3) of sub-semi-rings: consider any $f \in P$, then $-f = (-1)f \in P$ by (3) of sub-semi-algebras.

- If $P \leq_{\mathrm{m}} M$ is a sub-module (of the R-module M, where $(R, +, \cdot)$ is a integral domain) then we obtain another sub-module of M by letting

$$\mathrm{Hull}(P) \;:=\; \{\, x \in M \mid \exists\, a \in R : a \neq 0 \text{ and } ax \in P \,\}$$

 Thereby $P \subseteq \mathrm{Hull}(P) \leq_{\mathrm{m}} M$ of course. Prob Clearly $p = 1 \cdot p \in \mathrm{Hull}(P)$ for any $p \in P$ such that $P \subseteq \mathrm{Hull}(P)$. In particular $0 \in \mathrm{Hull}(P)$ which is property (1). In (3) we are given $u \in R$ and $x \in \mathrm{Hull}(P)$. That is $ax \in P$ for some $a \neq 0$. Then $a(ux) = (au)x = (ua)x = u(ax) \in P$ such that $ux \in \mathrm{Hull}(P)$. Likewise, if $x, y \in \mathrm{Hull}(P)$ then ax and $by \in P$ for some $a, b \in R$ with $a, b \neq 0$. Now $ab(x + y) = (ab)x + (ab)y = b(ax) + a(by) \in P$. But as R is an integral domain we have $ab \neq 0$, as well and thereby $x + y \in \mathrm{Hull}(P)$, which is property (2).

- If A is an R-(semi-)algebra over some ring $(R, +, \cdot)$ then the center $\mathrm{cen}(A) \subseteq A$ (i.e. the elements of A that commute with all other elements) is an R-sub-(semi-)algebra of A again

$$\mathrm{cen}(A) \;=\; \{\, f \in A \mid \forall\, g \in A : fg = gf \,\} \quad \leq_{\mathrm{b}} A$$

 Prob Clearly $0 \in \mathrm{cen}(A)$ as for any $g \in A$ we have $0g = 0 = g0$ and if $a \in R$, $f, f' \in \mathrm{cen}(A)$ then we get $(af)g = a(fg) = f(ag) = (ag)f = a(gf) = g(af)$ and $(f + f')g = fg + f'g = gf + gf' = g(f + f')$ such that af and $f + f' \in \mathrm{cen}(A)$ again. Also $(ff')g = f(f'g) = f(gf') = (fg)f' = (gf)f' = g(ff')$ implies $ff' \in \mathrm{cen}(A)$. Altogether $\mathrm{cen}(A) \leq_{\mathrm{b}} A$ and if $1 \in A$ is the unit element then $1g = g = g1$ for any $g \in A$ such that $1 \in \mathrm{cen}(A)$ again.

- Let A be an R-semi-algebra over the ring $(R, +, \cdot)$, then $\mathfrak{a}$ is an algebra ideal of A iff it is an ideal and R-sub-semi-algebra of A, formally

$$\mathfrak{a} \trianglelefteq_{\mathrm{a}} A \quad \Longleftrightarrow \quad \mathfrak{a} \leq_{\mathrm{b}} A \text{ and } \mathfrak{a} \trianglelefteq_{\mathrm{i}} A$$

 Prob The implication $\Longleftarrow$ is clear: (M) of algebra-ideals is identical to (M) of sub-semi-algebras and (I) of algebra ideals just combines (4) and (5) of ideals. Conversely we first check property (4) of sub-semi-algebras: if $f, g \in \mathfrak{a}$, then in particular $g \in A$ and hence $fg \in \mathfrak{a}$ by (4) of algebra-ideals. Now properties (1) and (2) of ideals are contained in (M) of algebra ideals ((4) and (5) are (I) again). Thus it only remains to check property (3) of ideals. But if $f \in \mathfrak{a}$ then, as before $-f = (-1)f \in \mathfrak{a}$ by property (3) of algebra-ideals.

- If A even is an R-algebra over the ring $(R, +, \cdot)$, then there is no difference between ideals and algebra-ideals of A, formally

$$\mathfrak{a} \trianglelefteq_{\mathrm{a}} A \quad \Longleftrightarrow \quad \mathfrak{a} \trianglelefteq_{\mathrm{i}} A$$

Prob We have already seen $\mathfrak{a} \trianglelefteq_{\mathsf{a}} A \implies \mathfrak{a} \trianglelefteq_{\mathsf{i}} A$ above. Further we have already argued that it only remains to check property (3) of algebra-ideals: thus consider any $a \in R$ and $f \in \mathfrak{a}$, then $a1 \in A$ (where $1 \in A$, as A is an R-algebra) and hence $af = (a1)f \in \mathfrak{a}$ by (I).

(3.10) Proposition: (viz. 749)
Fix any ring $(R, +, \cdot)$ and for the moment being let $\star$ appreviate any one of the words *R-module*, *R-semi-algebra* or *R-algebra* and let M be a $\star$. Further consider an arbitrary family (where $i \in I \neq \emptyset$) $P_i \subseteq M$ of sub-$\star$s of M. Then the intersection of the P_i is a sub-$\star$ again

$$\bigcap_{i \in I} P_i \quad \subseteq \quad M \quad \text{is a sub-}\star$$

Likewise let A be an R-semi-algebra and let $\mathfrak{a}_i \trianglelefteq_{\mathsf{a}} A$ be an arbitrary (that is $i \in I \neq \emptyset$ again) family of R-algebra-ideals of A, then the intersection of the $\mathfrak{a}_i$ is an R-algebra-ideal of A again

$$\bigcap_{i \in I} \mathfrak{a}_i \quad \trianglelefteq_{\mathsf{a}} \quad A \quad \text{is an } R\text{-algebra-ideal}$$

(3.11) Definition:
Fix any ring $(R, +, \cdot)$ again, let $\star$ abbreviate any one of the words *R-module*, *R-semi-algebra* or *R-algebra* again and let M be a $\star$. If $X \subseteq M$ is an arbitrary subset then we define the **linear hull** $\mathrm{Lh}(X)$ resp. $\mathrm{Lh}_R(X)$ of X to be the following subset of M: If $X = \emptyset$, then we let $\mathrm{Lh}(\emptyset) := \{0\}$ and for $X \neq \emptyset$ we take to

$$\mathrm{Lh}(X) \quad = \quad \left\{ \sum_{i=1}^{n} a_i x_i \;\middle|\; 1 \leq n \in \mathbb{N},\, a_i \in R,\, x_i \in X \right\} \quad \subseteq \quad M$$

And the $\star$ **generated** by X is the intersection of all sub-$\star$s containing X:

$$\begin{aligned} \langle X \rangle_{\mathsf{m}} &:= \bigcap \{\, P \subseteq M \mid X \subseteq P \leq_{\mathsf{m}} M \,\} \\ \langle X \rangle_{\mathsf{b}} &:= \bigcap \{\, P \subseteq M \mid X \subseteq P \leq_{\mathsf{b}} M \,\} \\ \langle X \rangle_{\mathsf{a}} &:= \bigcap \{\, P \subseteq M \mid X \subseteq P \leq_{\mathsf{a}} M \,\} \end{aligned}$$

Nota in case there is any doubt concerning the module X is contained in, (e.g. $X \subseteq M \subseteq N$) we emphasize the R-module M used in this construction by writing $\langle X \subseteq M \rangle_{\mathsf{m}}$ or $\langle X \rangle_{\mathsf{m}} \leq_{\mathsf{m}} M$ and in literature there even is the notation $M\langle X \rangle_{\mathsf{m}}$, for the sub-module generated in M.

(3.12) Proposition: (viz. 749)
Fix any ring $(R, +, \cdot)$ and consider an R-module M containing the non-empty subset $X \subseteq M$, $X \neq \emptyset$. Then the sub-module generated by X is precisely the linear hull of X in M, formally

$$\langle X \rangle_{\mathsf{m}} \quad = \quad \left\{ \sum_{i=1}^{n} a_i x_i \;\middle|\; 1 \leq n \in \mathbb{N},\, a_i \in R,\, x_i \in X \right\}$$

And if A is an R-semi-algebra, $X \subseteq A$, $X \neq \emptyset$, then we can also describe the R-sub-semi-algebra generated by X explicitly. Namely we get the following description of this semi-algebra

$$\langle X \rangle_{\mathsf{b}} \;=\; \left\{ \sum_{i=1}^{n} a_i \prod_{j=1}^{m} x_{i,j} \;\middle|\; 1 \leq m,n \in \mathbb{N},\ a_i \in R,\ x_{i,j} \in X \right\}$$

Finally if A is an R-algebra, then the sub-algebra generated by X becomes $\langle X \rangle_{\mathsf{a}} = \langle X \cup \{1\} \rangle_{\mathsf{b}}$. And in the light of the explicit description above, we conclude that

$$\langle X \rangle_{\mathsf{a}} \;=\; \left\{ \sum_{i=1}^{n} a_i \prod_{j=1}^{m} x_{i,j} \;\middle|\; 1 \leq m,n \in \mathbb{N},\ a_i \in R,\ x_{i,j} \in X \cup \{1\} \right\}$$

(3.13) Remark:
In general the union $M \cup N$ of two modules need not be a module again, as it need not be closed under addition $+$. There is an important situation when this is the case, however: Let $(R,+,\cdot)$ be any ring, M be an R-module and for any $i \in I$ (where $I \neq \emptyset$) let $P_i \leq_{\mathsf{m}} M$ be sub-module of M. If the P_i form a *chain* - that is for any $i, j \in I$ we have $P_i \subseteq P_j$ or $P_j \subseteq P_i$ then the union

$$P \;:=\; \bigcup_{i \in I} P_i \quad \leq_{\mathsf{m}} \quad M$$

is a sub-module of M again. Likewise if A is an R-(semi)-algebra and for any $i \in I$ we have a sub-(semi)-algebra $P_i \leq_{\mathsf{b}} A$ of A, then their union *is* a sub-(semi)-algebra again

$$P \;:=\; \bigcup_{i \in I} P_i \quad \leq_{\mathsf{b}} \quad A$$

Prob As $I \neq \emptyset$ we have $0 \in P_i \subseteq P$ for any $i \in I$. Now consider $x, y \in P$ that is there are some $i, j \in I$ such that $x \in P_i$ and $y \in P_j$. As the P_i form a chain, we may assume $P_i \subseteq P_j$ without loss of generality. That is $x \in P_j$ as well and as P_j is a sub-module of M we hence get $ay \in P_j \subseteq P$ (for any $a \in R$) and $x + y \in P_j \subseteq P$ again. For the same reason, if the $P_i \leq_{\mathsf{b}} A$ are sub-(semi)-algebras of A, then the product $xy \in P_j \subseteq A$ is contained in P again.

3.2 First Concepts

In this and the following section we will introduce three separate concepts, that are all of fundamental importance. First we will introduce quotient modules - we have already studied quotient rings in (1.62), now we will generalize this concept to modules. Secondly we will turn our attention to torsion and annihilation. This is an important concept when it comes to analyzing the structure of a module, but will not occur in linear algebra. And finally we will introduce direct sums and products - the major tool for composing and decomposing modules over a common base ring.

(3.14) Definition: (viz. 750)
Let $(R,+,\cdot)$ be an arbitrary ring, consider an R-module M an R-sub-module $P \leq_{\mathsf{m}} M$ of M, then P induces an equivalence relation on M, by

$$x \sim y \quad :\Longleftrightarrow \quad y - x \in P$$

where x, $y \in M$. The equivalence classes under this relation are called **cosets** of P. For any $x \in M$ these are of the following form

$$x + P \;:=\; [x] \;=\; \{\, x + p \mid p \in P \,\}$$

Finally we denote the quotient set M modulo P to be the quotient set of M under this equivalence relation $\sim$. That is M/P is the set of all cosets, we denote it by

$$M \Big/ P \;:=\; M \Big/ \sim \;=\; \{\, x + P \mid x \in M \,\}$$

And thereby M/P can be turned into an R-module $(M/P,+,\diamond)$ again under the following operations

$$\begin{aligned} (x+P)+(y+P) &:= (x+y)+P \\ a \diamond (x+P) &:= (ax)+P \end{aligned}$$

Thereby $(M/P,+,\diamond)$ is also called the **quotient module** or **residue module** of M modulo P. Now consider an R-semi-algebra A and an R-algebra-ideal $\mathfrak{a} \trianglelefteq_{\mathsf{a}} A$. Then $A/\mathfrak{a}$ (in the sense above) not only is an R-module, but even becomes an R-semi-algebra $(A/\mathfrak{a},+,\cdot,\diamond)$, under the multiplication

$$(f+\mathfrak{a})(g+\mathfrak{a}) \;:=\; (fg)+\mathfrak{a}$$

Thereby $(A/\mathfrak{a},+,\cdot,\diamond)$ is also called the **quotient algebra** or **residue algebra** of A modulo $\mathfrak{a}$. And if A even is an R-algebra, then $(A/\mathfrak{a},+,\cdot,\diamond)$ is an R-algebra again, its unit element being given by $1+\mathfrak{a}$.

(3.15) Remark:
If $(R,+,\cdot)$ is any ring, then R is an R-module (even an R-algebra in case of a commutative ring) again (see above). And the property that $\mathfrak{a} \leq_{\mathsf{m}} R$ is a sub-module is precisely the same, as being a left-ideal. By the above definition $R/\mathfrak{a}$ thereby is an R-module again under the operations

$$(a+\mathfrak{a})+(b+\mathfrak{a}) \;=\; (a+b)+\mathfrak{a}$$

$$a \diamond (b + \mathfrak{a}) \quad = \quad (ab) + \mathfrak{a}$$

(3.16) Proposition: (viz. 750)
Correspondence Theorem: Let $(R, +, \cdot)$ be an arbitrary ring, M be an R-module and $L \leq_{\mathfrak{m}} M$ be any R-sub-module of M. Then we obtain the following correspondence of sub-modules

(i) Consider some R-sub-module $P \leq_{\mathfrak{m}} M$ such that $L \subseteq P$, then we obtain an R-sub-module P/L of the quotient module M/L by virtue of

$$P \Big/ L \quad := \quad \{ p + L \mid p \in P \} \quad \leq_{\mathfrak{m}} \quad M \Big/ L$$

and thereby for any element $x \in M$ we obtain the following equivalence for the *element of* relation

$$x + L \in P \Big/ L \quad \Longleftrightarrow \quad x \in P$$

(ii) Now the R-sub-modules of M/L correspond to the R-sub-modules of M containing L and this correspondence can be explicitly given to be

$$\begin{array}{rcl} \mathrm{Subm}\left(M \Big/ L\right) & \longleftrightarrow & \{ P \in \mathrm{Subm}(M) \mid L \subseteq P \} \\ U & \mapsto & \{ x \in M \mid x + L \in U \} \\ P \Big/ L & \hookleftarrow & P \end{array}$$

(iii) Consider an arbitrary family $P_i \leq_{\mathfrak{m}} M$ (where $i \in I$) of R-sub-modules of M such that for any $i \in I$ we get $L \subseteq P_i$. Then the intersection commutes with taking to quotients, that is we obtain

$$\bigcap_{i \in I} \left(P_i \Big/ L \right) \quad = \quad \left(\bigcap_{i \in I} P_i \right) \Big/ L$$

(iv) As in (iii) consider any $P_i \leq_{\mathfrak{m}} M$ where $i \in I$ and $L \subseteq P_i$, then the summation also commutes with taking to quotients, that is

$$\sum_{i \in I} \left(P_i \Big/ L \right) \quad = \quad \left(\sum_{i \in I} P_i \right) \Big/ L$$

(v) More generally consider any family of sumbodules $P_i \leq_{\mathfrak{m}} M$ (where $i \in I$) such that $L \subseteq \sum_i P_i$, then we obtain the following identity

$$\sum_{i \in I} \left(P_i + L \Big/ L \right) \quad = \quad \left(\sum_{i \in I} P_i \right) \Big/ L$$

(vi) Finally for any subset $X \subseteq M$ let us denote $X/L := \{ x + L \mid x \in X \}$ that is $X/L \subseteq M/L$, then we obtain the following identity

$$\langle X \Big/ L \rangle_{\mathfrak{m}} \quad = \quad \langle X \rangle_{\mathfrak{m}} + L \Big/ L$$

(3.17) Proposition: (viz. 752) **Modular Rule**
Let $(R,+,\cdot)$ be an arbitrary ring, M be an R module and P, Q and $U \leq_{\mathfrak{m}} M$ be R-sub-modules of M such that $P \subseteq Q$. Then we obtain

$$(Q \cap U) + P \;=\; Q \cap (P + U)$$

$$P \cap U = Q \cap U,\; P + U = Q + U \;\Longrightarrow\; P = Q$$

(3.18) Proposition: (viz. 865)
Let $(R,+,\cdot)$ be an arbitrary ring and N be an R-module. Further consider a cofinite sub-module $P \leq_{\mathfrak{m}} N$ of N, that is there are some $x_1,\ldots,x_n \in N$ such that we have the equality

$$P + \mathsf{Lh}\{\, x_1,\ldots,x_n \,\} \;=\; N$$

If further $P \neq N$, then there is a maximal sub-module M of N containing P. That is $M \leq_{\mathfrak{m}} N$ is a sub-module satisfying the following three properties

(1) $M \neq N$

(2) $P \subseteq M \subseteq N$

(3) $\forall\, Q \leq_{\mathfrak{m}} N$ we get $M \subseteq Q \subseteq N \implies M = Q$ or $M = N$

(3.19) Remark:
In (3.110) we will see, that $\mathbb{Q}$ (regarded as a $\mathbb{Z}$-module) does not have a single maximal sub-module. No wonder, that we also found $\mathbb{Q}$ to be ininitely generated: If it was finitely generated then by the proposition above there would be a maximal module containing $\{0\}$.

(3.20) Definition:
Let $(R,+,\cdot)$ be any ring and M be an R-module. Further consider an element $x \in M$ and an arbitrary subset $X \subseteq M$, then we introduce

(i) We define the **annihilator** of x to be the subset of elements of R, that multiply x to zero. Likewise the annihilator of X is the subset of elements of R that multiply all $x \in X$ to zero, simultaneously

$$\begin{aligned}
\mathsf{ann}(x) &:= \{\, a \in R \mid ax = 0 \,\} \\
\mathsf{ann}(X) &:= \{\, a \in R \mid \forall\, x \in X : ax = 0 \,\} \\
&= \bigcap_{x \in X} \mathsf{ann}(x)
\end{aligned}$$

If we want to emphasize the base ring in which the annihilator is generated, we also write $\mathsf{ann}_R(X)$ instead of $\mathsf{ann}(X)$. It is easy to see that any annihilator $\mathsf{ann}(X)$ is a left-ideal in R. Finally the set of all left-ideals of R occuring as annihilators of non-zero elements of M will be denoted by

$$\mathsf{Anns}(M) \;:=\; \{\, \mathsf{ann}(x) \mid x \in M,\; x \neq 0 \,\}$$

(ii) For $X \subseteq \{0\}$ we let $\mathrm{zd}_R(X) := \{0\}$ and if there is some $x \in X$ with $x \neq 0$ then we define the set of **zero-divisors** of X to be the subset of elements of R that multiply a non-zero $x \in X$ to zero

$$\mathrm{zd}_R(X) \;:=\; \{\, a \in R \mid \exists\, x \in X \;:\; x \neq 0 \text{ and } ax = 0 \,\} \;=\; \bigcup_{0 \neq x \in X} \mathrm{ann}(x)$$

(iii) The complement of the zero-divisors is called the set of **non-zero-divisors** of X, which we denote by $\mathrm{nzd}_R(X) := R \setminus \mathrm{zd}_R(X)$. And if there is some $x \in X$ with $x \neq 0$ then this set is given to be

$$\begin{aligned} \mathrm{nzd}_R(X) \;&:=\; R \setminus \mathrm{zd}_R(X) \\ &=\; \{\, a \in R \mid \forall\, x \in X \;:\; x \neq 0 \implies ax \neq 0 \,\} \\ &=\; \{\, a \in R \mid \forall\, x \in X \;:\; ax = 0 \implies x = 0 \,\} \end{aligned}$$

(iv) We thereby define the **torsion sub-module** of M to be the collection of elements of M that have an non-trivial annihilator (i.e. $ax = 0$ for some $a \neq 0$), formally that is

$$\begin{aligned} \mathrm{tor}(M) \;&:=\; \{\, x \in M \mid \exists\, a \in R : a \neq 0 \text{ and } ax = 0 \,\} \\ &=\; \{\, x \in M \mid \mathrm{ann}(x) \neq 0 \,\} \end{aligned}$$

If $x \in \mathrm{tor}(M)$ then x is said to be a **torsion element** of M. And M is said to be a **torsion module** iff $\mathrm{tor}(M) = M$ and M is said to be **torsion-free** (or **faithful**) iff $\mathrm{tor}(M) = \{0\}$. In other words that is: M is torsion-free, iff for any $a \in R$ and $x \in M$ we have the implication

$$ax \;=\; 0 \quad\Longrightarrow\quad a \;=\; 0 \;\text{ or }\; x \;=\; 0$$

Prob If M is torsion-free, suppose $ax = 0$: If $a = 0$ we are done, hence consider the case $a \neq 0$. By definition this is $x \in \mathrm{tor}(M) = \{0\}$ and hence $x = 0$. Conversely, if the implication holds, then $x \in \mathrm{tor}(M)$ implies $x =$ and hence $\mathrm{tor}(M) = \{0\}$.

(v) A sub-module $P \leq_{\mathsf{m}} M$ is said to be a **pure** sub-module of M, iff it satisfies one of the following three equivalent conditions

(a) $\mathrm{tor}(M/P) = \{\, 0 + P \,\}$

(b) $\mathrm{Hull}(P) = P$

(c) for any $a \in R$ with $a \neq 0$ and any $x \in M$ we get the implication

$$ax \in P \quad\Longrightarrow\quad x \in P$$

Prob for any $x \in M$ we have $x + P \in \mathrm{tor}(M/P)$ if and only if there is some $a \in R$ with $a \neq 0$ such that $a(x + P) = 0 + P$ and this again is $ax \in P$. Hence M/P is torsion-free if and only if $ax \in P$ implies $x + P = 0 + P$, which in turn is $x \in P$. So (a) and (c) are equivalent. Now $P \subseteq \mathrm{Hull}(P)$ is true in general and (c) is nothing but $\mathrm{Hull}(P) \subseteq P$, such that (c) also is equivalent to (b).

(3.21) Example:
Let $(R,+,\cdot)$ be any ring and $\mathfrak{a} \trianglelefteq_{\mathsf{i}} R$ be an ideal of R. Considering $M := R/\mathfrak{a}$ as an R-module we find the annihilator of M to be $\mathfrak{a}$ again

$$\operatorname{ann}\left(R\Big/_{\mathfrak{a}}\right) \;=\; \mathfrak{a}$$

Prob If $a \in \operatorname{ann}(R/\mathfrak{a})$ then in particular $0+\mathfrak{a} = 0 = a(1+\mathfrak{a}) = a+\mathfrak{a}$ such that $a \in \mathfrak{a}$. Conversely if $a \in \mathfrak{a}$ and $b+\mathfrak{a} \in R/\mathfrak{a}$ then $ab \in \mathfrak{a}$, as $\mathfrak{a}$ is an ideal. But this means $0 = 0+\mathfrak{a} = ab+\mathfrak{a} = a(b+\mathfrak{a})$.

(3.22) Proposition: (viz. 752)
Let $(R,+,\cdot)$ be any ring, M be an R-module and $X \subseteq M$ be an arbitrary subset of M. Then we obtain all of the following statements

(i) The annihilator of an arbitrary set X is a left-ideal of R, the annihilator of some sub-module $P \leq_{\mathsf{m}} M$ even is an ideal of R, formally that is

$$\begin{aligned} \operatorname{ann}(X) &\leq_{\mathsf{m}} R \\ \operatorname{ann}(P) &\trianglelefteq_{\mathsf{i}} R \end{aligned}$$

(ii) ($\diamondsuit$) Let $x \in M$ be any element of the R-module M and recall that the R-sub-module of M generated by $\{x\}$ is given to be $Rx = \{ax \mid a \in R\}$. Then we obtain the following isomorphy of R-modules

$$R\Big/_{\operatorname{ann}(x)} \;\cong_{\mathsf{m}}\; Rx \;:\; b+\operatorname{ann}(x) \;\mapsto\; bx$$

In particular: If $\mathfrak{a} \trianglelefteq_{\mathsf{i}} R$ is a proper ($\mathfrak{a} \neq R$) ideal, then it also is an annihilator $\mathfrak{a} = \operatorname{ann}(x)$ of some $x \in M$ iff there is a monomorphism ι of R-modules that maps $R/\mathfrak{a}$ into M

$$\mathfrak{a} \in \operatorname{Anns}(M) \iff \exists\, \iota : R\Big/_{\mathfrak{a}} \hookrightarrow M$$

(iii) Let $(S,+,\cdot)$ be a skew-field and M be an S-module, if now $0 \neq x \in M$ is a non-zero element of M, then the annihilator of x is 0. In particular M is torsion free and $S \xrightarrow{\sim} Sx : a \mapsto ax$ is an isomorphism of S-modules

$$\operatorname{ann}(x) \;=\; \begin{cases} S \text{ if } x = 0 \\ 0 \text{ if } x \neq 0 \end{cases}$$

(iv) Suppose R is a commutative ring, then the annihilator of X equals the annihilator of the R-sub-module generated by X, formally that is

$$\operatorname{ann}(X) \;=\; \operatorname{ann}\Big(\langle X\rangle_{\mathsf{m}}\Big)$$

Consequently if $\{x_i \mid i \in I\} \subseteq M$ is a set of generators of the R-module $M = \operatorname{Lh}\{x_i \mid i \in I\}$ then the annihilator of M is just

$$\operatorname{ann}(M) \;=\; \bigcap_{i\in I} \operatorname{ann}(x_i)$$

($\diamondsuit$) And the R-module homomorphism $\varphi : R \to M^I$ defined by $\varphi(a) := (ax_i)$ has the kernel $\mathrm{kn}(\varphi) = \mathrm{ann}(M)$. In particular we obtain an embedding (i.e. an injective R-module homomorphism)

$$R \Big/ \mathrm{ann}(M) \hookrightarrow M^I \ : \ a + \mathrm{ann}(M) \mapsto (ax_i)$$

(v) If $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ is an ideal contained in the annihilator ideal $\mathfrak{a} \subseteq \mathrm{ann}(M)$ of M, then M can be turned into a $(R/\mathfrak{a})$-module using the following scalar-multiplication (where $a \in R$ and $x \in M$)

$$(a + \mathfrak{a})x \ := \ ax$$

(3.23) Proposition: (viz. 754)
Let $(R, +, \cdot)$ be any non-zero ring $R \neq 0$ and M be an R-module. Then we obtain the following statements

(i) If R is a integral domain, then the torsion sub-module $\mathrm{TOR}(M)$ truly is an R-sub-module of M

$$\mathrm{TOR}(M) \quad \leq_{\mathrm{m}} \quad M$$

and the quotient module of M modulo $\mathrm{TOR}(M)$ is torsion-free, put formally that is the equation

$$\mathrm{TOR}\left(M \Big/ \mathrm{TOR}(M)\right) \ = \ \{0\}$$

(ii) If R is an integral domain, M is a free R-module and $P \leq_{\mathrm{m}} M$ is any sub-module of M, then P already is torsion-free. Formally again

$$R \text{ integral domain, } M \text{ free} \implies \mathrm{TOR}(P) = 0$$

(iii) If $R \neq 0$ and $M \neq 0$ both are non-zero, then the following statements are equivalent (recall that in this case M was said to be *torsion-free*, resp. *faithful*)

(a) $\mathrm{ZD}_R(M) \subseteq \{0\}$

(b) $\mathrm{TOR}(M) = \{0\}$, where $0 \in M$

(c) $\mathrm{Anns}(M) = \{0\}$, where $0 = \{0\} \subseteq R$

(d) $\forall\, a \in R, \forall\, x \in M$ we get $ax = 0 \implies a = 0$ or $x = 0$

Nota if $M = 0$, then (a) and (d) are true, (b) is equivalent to $R \neq 0$, yet (c) is false, as $\mathrm{Anns}(M) = \emptyset$.

(iv) If M is a finitely generated module over the integral domain R, then the following two properties of M are equivalent

(a) M is torsion-free

(b) There is some $n \in \mathbb{N}$ such that M can be embedded into R^n. That is there is some monomorphism μ of R-modules of the form

$$\mu \ : \ M \ \hookrightarrow \ R^n$$

(v) ($\diamondsuit$) If N is another R-module and $\Phi : M \xrightarrow{\sim} N$ an isomorphism of R-modules, then we get $\Phi(\mathrm{tor}(M)) = \mathrm{tor}(N)$ and thereby obtain the following isomorphies of R-modules

$$\begin{aligned} \mathrm{tor}(M) &\xrightarrow{\sim} \mathrm{tor}(N) \quad : \quad x \mapsto \Phi(x) \\ M\big/_{\mathrm{tor}(M)} &\xrightarrow{\sim} N\big/_{\mathrm{tor}(N)} \quad : \quad x + \mathrm{tor}(M) \mapsto \Phi(x) + \mathrm{tor}(N) \end{aligned}$$

(vi) If $M \neq 0$ is a finitely generated, non-zero, torsion-free $\mathrm{tor}(M) = 0$ R-module, then M contains a maximal pure sub-module, formally this can be put as

$$\{\, P \leq_{\mathfrak{m}} M \mid P \neq M,\, P \text{ is pure} \,\}^* \neq \emptyset$$

(3.24) Proposition: (viz. 756)
Let $(R, +, \cdot)$ be a commutative ring and M be any R-module. Then we obtain the following statements

(i) If M is a simple, non-zero R-module, then the annihilator of M is a maximal ideal of R, formally

$$\mathrm{ann}(M) \in \mathrm{Smax}(R)$$

(ii) If $x \in M$ is any element of M, then $\mathrm{ann}(x)$ is a prime ideal if and only if for any $a \in R$ we either have $ax = 0$ or $\mathrm{ann}(ax) = \mathrm{ann}(x)$. That is the following two statements are equivalent

(a) $\mathrm{ann}(x)$ is a prime ideal of R

(b) $\forall\, a \in R$ we get $\mathrm{ann}(ax) = R$ or $\mathrm{ann}(ax) = \mathrm{ann}(x)$

(iii) Let $x \in M$ be any element of M, such that $\mathfrak{p} := \mathrm{ann}(x) \in \mathrm{Spec}(R)$ is a prime ideal of R. Then for any $a \in R \setminus \mathfrak{p}$ and $y := ax$ the sub-module $Ry \leq_{\mathfrak{m}} M$ only has a single annihilator ideal

$$\mathrm{Anns}(Ry) = \{\, \mathfrak{p} \,\}$$

(iv) If $R \neq 0$ is non-zero, then maximal annihilator ideals of M are prime ideals of R. Formally that is

$$\big(\mathrm{Anns}(M)\big)^* \subseteq \mathrm{Spec}(R)$$

(3.25) Definition: (viz. 757)
Let $(R, +, \cdot)$ be any ring and M be an R-module. Also let $P, Q \leq_{\mathfrak{m}} M$ be any two sub-modules of M, then we define the **ideal quotient** $Q : P$ to be the following subset of R

$$Q : P := \{\, a \in R \mid aP \subseteq Q \,\} \leq_{\mathfrak{m}} R$$

Nota thereby $Q : P \leq_{\mathfrak{m}} R$ is an R-sub-module of R and also we get $\mathrm{ann}(M) = 0 : M$. In particular, if R is commutative $Q : P \trianglelefteq_{\mathfrak{i}} R$ truly is an ideal, as the name suggests and in this case we also get $\mathrm{ann}(x) = 0 : Rx$ for any $x \in M$.

3.3 Direct Sums

(3.26) Definition:
Let $(R,+,\cdot)$ be an arbitrary ring and consider an R-module M. If we are given finitely many sub-modules $P_1,\dots,P_n \leq_{\mathfrak{m}} M$ of M, then we define their **sum** to be set of all sums of elements of the P_i

$$P_1+\cdots+P_n \;:=\; \{\, x_1+\cdots+x_n \mid x_i\in P_i \,\}$$

If we are given an arbitrary collection of R-sub-modules $P_i \leq_{\mathfrak{m}} M$, where $i\in I$ is any index set, then we generalize the finite case directly by defining the **sum** of the P_i to be the set of all *finite* sums of elements of the P_i, that is

$$\sum_{i\in I} P_i \;:=\; \bigcup_{n=1}^{\infty} \left\{ x_1+\cdots+x_n \;\middle|\; \{\, i(1),\dots,i(n)\,\}\subseteq I,\; x_k\in P_{i(k)} \right\}$$

By definition this set consists of finite sums of elements $x_1+\cdots+x_n$ where $x_k\in P_{i(k)}$ for some $i(k)\in I$. Thus if we denote the collection of finite subsets of I by $\mathcal{I}:=\{\,\Omega\subseteq I \mid \#\Omega<\infty\,\}$ then we may present a slightly more formal description of this set

$$\sum_{i\in I} P_i \;=\; \left\{ \sum_{i\in\Omega} x_i \;\middle|\; \Omega\in\mathcal{I},\; x_i\in P_i \right\}$$

(3.27) Remark:

(i) Suppose we are given a collection of elements $(x_i)\subseteq M$ such that for any $i\in I$ we have $x_i\in P_i$. More importantly suppose that among these x_i only finitely many are non-zero, that is the set $\Omega:=\{\,i\in I \mid x_i\neq 0\,\}$ is finite. As in (1.26) we then denote

$$\sum_{i\in I} x_i \;:=\; \sum_{i\in\Omega} x_i$$

That is: If only finitely many of the x_i are non-zero, then there is a well-defined notion of the sum of these elements - just leave out the zeros and sum up these (finitely many) non-zero elements.

(ii) It is clear that $P_1+\cdots+P_n$ and - more generally - $\sum_i P_i$ are sub-modules of M. Prob Given any $x=\sum_i x_i$ and $y=\sum_i y_i\in\sum_i P_i$ their sum is $x+y=\sum_i(x_i+y_i)$ and as P_i is a sub-module this means $x_i+y_i\in P_i$ and hence $x+y\in\sum_i P_i$ again. Likewise for any $a\in R$ we have $ax=\sum_i(ax_i)\in\sum_i P_i$, as also $ax_i\in P_i$.

(iii) In fact, in the light of proposition (3.12) this is just the R-sub-module of M generated by the P_i, i.e. $P_1+\cdots+P_n=\langle P_1\cup\cdots\cup P_n\rangle_{\mathfrak{m}}\leq_{\mathfrak{m}} M$. More generally: Given an arbitrary collection of R-sub-modules $P_i\leq_{\mathfrak{m}} M$, where $i\in I$ is any index set, then the sum of the P_i is just the sub-module generated by the union of all the P_i

$$\sum_{i\in I} P_i \;=\; \langle \bigcup_{i\in I} P_i\rangle_{\mathfrak{m}}$$

(iv) In particular, if $x \in M$ is any single element, then the sub-module $\langle\{ x \}\rangle_{\mathsf{m}}$ of M generated by x is $\langle\{ x \}\rangle_{\mathsf{m}} = \mathrm{Lh}_R\{ x \} = Rx := \{ ax \mid a \in R \}$. Generally for any $x_1, \ldots, x_n \in M$ the R-linear hull is just the set of all linear combinations $a_1x_1 + \cdots + a_nx_n \in M$ for some $a_1, \ldots, a_n \in R$

$$\mathrm{Lh}_R\{ x_1, \ldots, n_n \} \quad = \quad Rx_1 + \cdots + Rx_n$$

Even more generally, as the R-linear hull and the sum of sub-modules are based on finite sums only, it is clear that for an arbitrary collection of elements $(x_i) \subseteq M$ the linear hull of the x_i is just the the sum of the sub-modules generated by the x_i, formally that is

$$\mathrm{Lh}_R\{ x_i \mid i \in I \} \quad = \quad \sum_{i \in I} Rx_i$$

(v) If we are given a chain (P_i) of sub-modules, that is $P_i \leq_{\mathsf{m}} M$ is a sub-module for any $i \in I$ such that for any $i, j \in I$ we have $P_i \subseteq P_j$ or $P_j \in P_i$, then even the union of the P_i itself (not only their sum) is a sub-module of M

$$\bigcup_{i \in I} P_i \quad \leq_{\mathsf{m}} \quad M$$

Prob consider $a \in R$ and $x, y \in P$ where we abbreviate $P = \bigcup_i P_i$. That is $x \in P_i$ and $y \in P_j$ for some i resp. $j \in I$. Without loss of generality we may assume $P_i \subseteq P_j$ and that is $x \in P_j$ as well. Then as P_i and $P_j \leq_{\mathsf{m}} M$ are sub-modules again we clearly have $ax \in P_i$ and $x + y \in P_j$ such that ax and $x + y \in P$ again. That is P truly is a sub-module of M again.

(3.28) Example:
Sadly the summation and intersection of modules do not fit together nicely. This is to say: if we are given sub-modules P and $Q_i \leq_{\mathsf{m}} M$ of an R-module M, then in general we only get

$$P + \bigcap_{i \in I} Q_i \quad \subseteq \quad \bigcap_{i \in I} (P + Q_i)$$

Yet the equality of these sets need not hold true. As an example we regard the ring $R := \mathbb{Z}$ and pick up the $\mathbb{Z}$-module $M := \mathbb{Z}$ again. If now $P := 2\mathbb{Z}$ and for any $i \in I = \{ i \in \mathbb{N} \mid i \geq 3, i \text{ prime} \}$ we let $Q_i := i\mathbb{Z}$, then it is clear, that $P + Q_i = M$ for any $i \in I$ [as $2\mathbb{Z} + i\mathbb{Z} = \gcd(2, i)\mathbb{Z} = \mathbb{Z}$ due to the lemma (2.83) of Bezout]. However if $x \in Q_i$ for any $i \in I$, then $i \mid x$, such that x would have infinitely many prime divisors. This forces $x = 0$ and hence the intersection $\bigcap_i Q_i = 0$. Therefore we only have

$$P + \bigcap_{i \in I} Q_i \quad = \quad 2\mathbb{Z} \quad \subset \quad \mathbb{Z} \quad = \quad \bigcap_{i \in I} (P + Q_i)$$

(3.29) Definition: (viz. 758)

- Let $(R, +, \cdot)$ be any ring, $I \neq \emptyset$ be a non-empty index set and for any $i \in I$ let M_i [more explicitly $(M_i, +, \diamond)$] be an R-module. Then we regard the cartesian product of the M_i

$$M \quad := \quad \prod_{i \in I} M_i$$

This can be turned into another R-module - called the **(exterior) direct product** of the M_i - by installing the following (point-wise) algebraic operations (where $x = (x_i)$, $y = (y_i) \in M$ and $i \in I$)

$$\begin{aligned} + &: M \times M \to M \quad : \quad (x,y) \mapsto (x_i + y_i) \\ \diamond &: R \times M \to M \quad : \quad (a,x) \mapsto (ax_i) \end{aligned}$$

Note that $x_i + y_i$ is the addition of vectors in M_i and ax_i is the scalar multiplication in M_i and hence these operations are well-defined. It is easy to see that M thereby inherits the properties of an R-module.

- We have just introduced the direct product M of the M_i as an R-module. Let us now define a certain R-sub-module of M, called the **(exterior) direct sum** of the M_i. To do this let us first denote the *support* of $x = (x_i) \in M$ to be $\mathrm{Supp}(x) := \{\, i \in I \mid x_i \neq 0 \in M_i \,\} \subseteq I$, i.e. the set of indexes i with non-vanishing x_i. Then we let

$$\bigoplus_{i\in I} M_i \;:=\; \left\{ x \in \prod_{i\in I} M_i \;\middle|\; \#\mathrm{Supp}(x) < \infty \right\}$$

That is $\bigoplus_i M_i$ consists of all the $x = (x_i) \in \prod_i M_i$ that contain finitely many non-zero coefficients $x_i \neq 0$ only. In particular the direct sum coincides with the direct product if and only if I is finite

$$\bigoplus_{i\in I} M_i \;=\; \prod_{i\in I} M_i \quad\Longleftrightarrow\quad \#I < \infty$$

Generally $\bigoplus_i M_i$ becomes an R-module again under the same algebraic operations that we have introduced for the direct product $\prod_i M_i$. Formally that is: The exterior direct sum is an R-sub-module of the exterior direct product

$$\bigoplus_{i\in I} M_i \quad \leq_{\mathsf{m}} \quad \prod_{i\in I} M_i$$

- If for any $i \in I \neq \emptyset$ we are even given an R-semi-algebra A_i then the (exterior) direct product $A := \prod_i A_i$ of the A_i is an R-semi-algebra again, under the point-wise multiplication

$$\cdot \;:\; A \times A \to A \;:\; (x,y) \mapsto (x_i y_i)$$

where, as before, $x_i y_i$ is the multiplication in A_i. Also the exterior direct sum $\oplus_i A_i$ of the A_i is a sub-semi-algebra of A again. And if for any $i \in I$ we even have an R-algebra A_i with unit element $1_i \in I$ then the exterior direct product $\prod_i A_i$ is an R-algebra, too having the unit element $1 = (1_i)$.

- $(\diamondsuit)$ Let now N be another R-module and for any $i \in I$ consider an R-module homomorphism $\varphi_i : M_i \to N$. Then we obtain a well-defined R-module-homomorphism from the direct sum to N

$$\bigoplus_{i\in I} \varphi_i \;:\; \bigoplus_{i\in I} M_i \to N \;:\; (x_i) \mapsto \sum_{i\in I} \varphi_i(x_i)$$

This is well-defined, as only finitely many $x_i \in M_i$ are non-zero [as (x_i) is contained in the direct *sum* of the M_i] and hence the sum only contains finitely many non-zero summands. And the properties of an R-module-homomorphism are trivially inherited from the φ_i.

- Now consider any R-module M and for any $i \in I$ an R-sub-module $P_i \leq_{\mathsf{m}} M$. And for any $j \in I$ let us denote by $\widehat{P}_j$ the R-sub-module generated by all P_i except P_j, formally we denote

$$\widehat{P}_j \;:=\; \sum_{i \neq j} P_i \;=\; \langle \bigcup_{i \in I \setminus \{j\}} P_i \rangle_{\mathsf{m}}$$

Then M is said to be the **(inner) direct sum** of the P_i iff the set $\{ P_i \mid i \in I \}$ of these sub-modules satisfies one of the following two equivalent statements

(a) The P_i build up M as their sum, but for any index $j \in I$ the intersection of P_j and its complement $\widehat{P}_j$ is trivial. Formally these are the statements

$$M = \sum_{i \in I} P_i \quad \text{and} \quad \forall\, j \in I : P_j \cap \widehat{P}_j = 0$$

(b) Any $x \in M$ has a representation as a (finite) sum of uniquely determined elements $x_i \in P_i$ (where $i \in I$). Formally this reads as

$$\forall\, x \in M \;\; \exists !\, (x_i) \in \prod_{i \in I} P_i \;\; : \;\; x = \sum_{i \in I} x_i$$

And in case that M is the inner direct sum ot the P_i we will use the following notation to express this fact (beware the similarity to the exterior direct sum above)

$$M \;=\; \bigoplus_{i \in I} P_i$$

- Let M be any R-module and $P \leq_{\mathsf{m}} M$ and R-sub-module again. Then P is said to be **complemented** or a **direct summand** of M, iff there is another sub-module $\widehat{P}$ of M, such that M is the inner direct sum of P and $\widehat{P}$. Formally that is: $\exists\, \widehat{P} \leq_{\mathsf{m}} M$ such that

(1) $M = P + \widehat{P}$
(2) $P \cap \widehat{P} = 0$

(3.30) Remark: (viz. 759)
Recall that in cartesian products (and the direct product has been defined as such) for any $j \in I$ there is a *canonical projection* π_j of the product $\prod_i M_i$ onto M_j. Thereby the projection π_j is defined, to be

$$\pi_j \;:\; \prod_{i \in I} M_i \to M_j \;:\; (x_i) \mapsto x_j$$

But in contrast to arbitrary cartesisan products we also find (for any $j \in I$) a *canonical embedding* ι_j into the direct sum (and product), by letting

$$\iota_j \;:\; M_j \to \bigoplus_{i \in I} M_i \;:\; x_j \mapsto (\delta_{i,j} x_j)$$

where $\delta_{i,j}x_j := x_j$ for $i = j$ and $\delta_{i,j}x_j := 0 \in M_i$ for $i \neq j$. Then it is clear that $\pi_j\iota_j = \mathbb{1}$ is the identity on M_j and in particular π_j is surjective and ι_j is injective. Further these maps are tightly interwoven with the structure of the direct product and sum respectively. To be precise, consider any $x = (x_i) \in \prod_i M_i$, then x is precisely the I-tuple of its projections

$$x \;=\; \Big(\pi_i(x)\Big)$$

On the other hand for any $x = (x_i) \in \bigoplus_i M_i$ we obtain another identity (note that the sum thereby is well-defined, as only finitely many x_i are non-zero, such that in truth the sum is a finite only)

$$x \;=\; \sum_{i\in I} \iota_i(x_i)$$

($\diamondsuit$) By definition of the operations on the direct product/sum it is also clear that both projection π_j and embedding ι_j are homomorphisms of R-modules, as the operations on the sum/product are component-wise.

(3.31) Example:
Consider any ring $(R, +, \cdot)$, the R-module $M := R^2$ and the sub-modules $P_1 := R(1,0) = \{\, (a,0) \mid a \in R \,\}$ and $P_2 := R(0,1) = \{\, (0,b) \mid b \in R \,\}$. Then clearly M is the inner direct sum of P_1 and P_2

$$M \;=\; P_1 \oplus P_2$$

To check whether M can be decomposed as a direct sum of some P_i it does *not* suffice to verify, that the intersection of the P_i is pairwise trivial. In the example above let $P_3 := R(1,1) = \{\, (a,a) \mid a \in R \,\}$. Then it is clear that $M = P_1 + P_2 + P_3$ and $P_i \cap P_j = 0$ for any $i \neq j \in 1 \ldots 3$, but M is *not* the inner direct sum of P_1, P_2 and P_3. In fact $x = (1,1) \in M$ has non-unique representations as $x = (1,0) + (0,1) \in P_1 + P_2$ and as $x = (1,1) \in P_3$.

(3.32) Example:
The most common example of a direct sum of modules is a simple multiple of a single module: To be precise, let $(R, +, \cdot)$ be some ring and consider an R-module M. Then for any non-empty set I we denote the product (resp. sum) of one copy of M for any $i \in I$ by

$$\begin{aligned} M^I \;&:=\; \prod_{i\in I} M \;&=\; \{\, (x_i) = x : I \to M : i \mapsto x_i \,\} \\ M^{\oplus I} \;&:=\; \bigoplus_{i\in I} M \;&=\; \Big\{\, (x_i) \in M^I \mid \{\, i \in I \mid x_i \neq 0 \,\} \text{ is finite} \,\Big\} \end{aligned}$$

The most important example is the case $M = R$ of the base ring itself. That is $R^{\oplus I}$ which consists of I identical copies of R. By definition the operations on M^I (and $M^{\oplus I}$) are component-wise, that is for any (x_i), $(y_i) \in M^I$ and any $a \in R$ we have

$$\begin{aligned} (x_i) + (y_i) \;&=\; (x_i + y_i) \\ a(x_i) \;&=\; (ax_i) \end{aligned}$$

A special case of this is M^n - here we take n identical copies of M, where $1 \leq n \in \mathbb{N}$ is any natural number. In the formal terms above this can be put as M^I, where the set is $I = 1 \ldots n$. As I is finite there is no difference between the direct sum and product

$$M^n \;:=\; M^{1\ldots n} \;=\; \prod_{i=1}^{n} M \;=\; \bigoplus_{i=1}^{n} M$$

$(\diamondsuit)$ The rest of this section will be devoted to studying the interaction of homorphisms of modules and direct sums, resp. to compare the structures of different direct sums using isomorphisms. While we only need the very basic notions of homorphisms of modules, these will be introduced in section 3.8 only. Thus the reader is asked to familiarize himself with homo- and isomorphisms beforehand.

(3.33) Remark:
There is a reason why we didn't bother to strictly separate exterior and inner direct products. The reason simply is: There is not much of a difference to begin with, any inner direct product already is an exterior direct product (up to isomorphy) and any exterior direct product can be reformulated as an interior direct product. We will give a precise formulation of this fact in the proposition below. Thus the distinction between inner and exterior is a purely set-theoretic one, it doesn't affect the algebra involved. This is why we do not bother that our formalism doesn't really distinguish between the interior and exterior direct sums - the difference is no structural one. (In general group theory there *will be* a difference, however).

(3.34) Proposition: (viz. 759)

(i) $(\diamondsuit)$ Let $(R, +, \cdot)$ be any ring, M be an R-module and $P_i \leq_{\mathfrak{m}} M$ be an arbitrary ($i \in I$) collection of R-sub-modules of M. If now M is the inner direct sum $M = \bigoplus_i P_i$ of the P_i, then M is already isomorphic (as an R-module) to the exterior direct sum of the P_i under the isomorphism

$$\bigoplus_{i\in I} P_i \;\cong_{\mathfrak{m}}\; M \quad : \quad (x_i) \mapsto \sum_{i\in I} x_i$$

(ii) Let $(R, +, \cdot)$ be any ring and M_i an arbitrary ($i \in I$) collection of R-modules. Now let $M := \bigoplus_i M_i$ be the exterior direct product of these modules and let $P_i := \iota_i(M_i) \leq_{\mathfrak{m}} M$ be the embedding of P_i into M. Then M is just the interior direct sum of the P_i put formally, that is

$$\bigoplus_{i\in I} M_i \;=\; \bigoplus_{i\in I} P_i$$

(3.35) Proposition: (viz. 760)
Let $(R, +, \cdot)$ be any ring and M be an R-module. For an arbitrary index set I and any $i \in I$ let $M_i \leq_{\mathfrak{m}} M$ be a sub-module, such that M is the inner direct product of the M_i

$$M \;=\; \bigoplus_{i\in I} M_i$$

For any $i \in I$ also let $P_i \leq_{\mathsf{m}} M_i$ be a sub-module of M_i and take P to be the sum of these. Then $P \leq_{\mathsf{m}} M$ is a sub-module of M, that also is the inner direct sum of the P_i, formally

$$P := \sum_{i\in I} P_i = \bigoplus_{i\in I} P_i$$

and we obtain an isomorphism of R-modules from the exterior direct sum of the quotient modules M_i/P_i to the quotient module M/P by virtue of

$$\bigoplus_{i\in I} M_i \Big/ P_i \xrightarrow{\sim} M \Big/ P \,:\, (x_i + P_i) \mapsto \left(\sum_{i\in I} x_i\right) + P$$

(3.36) Remark:
If $P \leq_{\mathsf{m}} M$ is a sub-module and $P_i := M_i \cap P$, then we always get the inclusion $\sum_i P_i \subseteq P$ however these need not be equal. Thus the above proposition cannot be reformulated starting with $P \leq_{\mathsf{m}} M$.

As an example regard $M = \mathbb{Q}^2$, then clearly $M = M_1 \oplus M_2$ where $M_1 = \mathbb{Q}(1,1)$ and $M_2 = \mathbb{Q}(1,-1)$. If now $P = \mathbb{Q} \times \{0\} \subseteq M$ then clearly $P_1 = M_1 \cap P = 0$ and $P_2 = M_2 \cap P = 0$. Thus we have $P_1 + P_2 \subset P$ and hence cannot apply the proposition above.

(3.37) Proposition: (viz. 760)
Let $(R, +, \cdot)$ be an arbitrary ring and let I and J be arbitrary index sets. For any $i \in I$ resp. $j \in J$ let M_i and N_j be R-modules. Then we obtain the following isomorphy of R-modules

$$\mathsf{mhom}\left(\bigoplus_{i\in I} M_i, \prod_{j\in J} N_j\right) \cong_{\mathsf{m}} \prod_{(i,j)\in I\times J} \mathsf{mhom}(M_i, N_j)$$

We can even give the above isomorphism explictly: let us denote the direct sum of the M_i by $M := \bigoplus_i M_i$ and the direct product of the N_j by $N := \prod_j N_j$. Further denote the canonical embedding $\iota_i : M_i \to M$ and the canonical projection $\pi_j : N \to N_j$. Then the isomorphy explictly reads as

$$\begin{array}{rcl} \mathsf{mhom}(M,N) & \cong_{\mathsf{m}} & \displaystyle\prod_{(i,j)\in I\times J} \mathsf{mhom}(M_i, N_j) \\ \varphi & \mapsto & \left(\pi_j \varphi \iota_i\right) \\ \left(\displaystyle\bigoplus_{i\in I} \varphi_{i,j}\right) & \mapsfrom & \left(\varphi_{i,j}\right) \end{array}$$

Let us explain this compact notation a bit: for any $(I \times J)$-tupel of homomorphisms $\varphi_{i,j} : M_i \to N_j$ the corresponding homomorphism $\varphi := (\bigoplus_i \varphi_{i,j}) = (\sum_i \varphi_{i,j}\pi_i)$ is explicitly given to be the following:

$$\varphi \,:\, M \to N \,:\, (x_i) \to \left(\sum_{i\in I} \varphi_{i,j}(x_i)\right)$$

(3.38) Remark:
Suppose we even have $(\varphi_{i,j}) \in \prod_i \bigoplus_j \mathrm{mhom}(M_i, N_j)$, that is for any $i \in I$ the set $\left\{ j \in J \mid \varphi_{i,j} \neq 0 \right\}$ is finite. Then the induced map φ even lies in $(\bigoplus_i \varphi_{i,j}) \in \mathrm{mhom}(\bigoplus_i M_i, \bigoplus_j N_j)$. The converse need not be true however, as an example regard $I = 0$, $J = \mathbb{N}$, $M = R^{\oplus\mathbb{N}}$ and $N_j = R$. As a homomorphism φ we choose the identity $\varphi = \mathbb{1} : R^{\oplus\mathbb{N}} \to R^{\oplus\mathbb{N}}$. Then φ induces the tuple $\mathbb{1} \mapsto (\pi_j)$, which has no finite support.

3.4 Ideal-induced Modules

In this short section we will introduce the concept of the sub-module $\mathfrak{a}M$ generated by an ideal $\mathfrak{a}$ of R. This is a way of passing on from a module M over a ring R to a related module over the quotient ring $R/\mathfrak{a}$. So as always with going to quotients, one tries to single out unnecessary complications, solve the problem in the reduced case and later lift it up again, solving the original problem. This is particularly useful in case the quotient ring $R/\mathfrak{m}$ is a field, i.e. $\mathfrak{m}$ is a maximal ideal.

While the construction is elementary it yields some very useful results - primarily the lemma of Nakayama. Though these results are of little value in their own right, they are powerful tools in providing proofs of more substantial theorems. Hence one might as well skip this section and postpone it, until one encounters the urge to use a quotient construction.

(3.39) Definition:
Consider an arbitrary ring $(R,+,\cdot)$, an ideal $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$ and an R-module M. Let further $P \leq_{\mathfrak{m}} M$ be a sub-module of M, then we denote the sub-module of M generated by elements of the form ap, for some $a \in \mathfrak{a}$ and $p \in P$, by

$$\mathfrak{a}P \;:=\; \langle \{\, ap \mid a \in \mathfrak{a},\ p \in P \,\} \rangle_{\mathfrak{m}}$$

(3.40) Proposition: (viz. 762)
Let $(R,+,\cdot)$ be an arbitrary ring, $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$ an ideal and consider a sub-module $P \leq_{\mathfrak{m}} M$ of the R-module M. Then we get the statements

(i) The sub-module $\mathfrak{a}P$ of M can be given explicitly, to be the following subset of M

$$\mathfrak{a}P \;=\; \left\{ \sum_{i=1}^{n} a_i p_i \;\middle|\; 1 \leq n \in \mathbb{N},\ a_i \in \mathfrak{a},\ p_i \in P \right\}$$

(ii) If P is generated by $\{\, p_j \mid j \in J \,\} \subseteq P$ (for some arbitrary index set J), then for any $x \in \mathfrak{a}P$ there are some $n \in \mathbb{N}$, some $a_1, \ldots, a_n \in \mathfrak{a}$ and $p_1, \ldots, p_n \in \{\, p_j \mid j \in J \,\}$ such that x can be written as

$$x \;=\; a_1 p_1 + \cdots + a_n p_n$$

If R is commutative and $\mathfrak{a}$ is generated by $\{\, a_i \mid i \in i \,\} \subseteq \mathfrak{a}$ (for some arbitrary index set I), then for any $x \in \mathfrak{a}P$ there are some $n \in \mathbb{N}$, some $a_1, \ldots, a_n \in \{\, a_i \mid i \in i \,\}$ and $p_1, \ldots, p_n \in P$ such that x can be written in the same way, as above.

(iii) Due to its definition $\mathfrak{a}P$ is a sub-module of P and thereby we obtain the following chain of inclusions

$$\mathfrak{a}P \quad \leq_{\mathfrak{m}} \quad P \quad \leq_{\mathfrak{m}} \quad M$$

(iv) Both the assignments $\mathfrak{a} \mapsto \mathfrak{a}P$ and $P \mapsto \mathfrak{a}P$ are order preserving, that is given any two ideals $\mathfrak{a}$ and $\mathfrak{b} \trianglelefteq_{\mathfrak{i}} R$ resp. any two sub-modules P and $Q \leq_{\mathfrak{m}} M$ we obtain the following implications

$$\mathfrak{a} \subseteq \mathfrak{b} \quad \Longrightarrow \quad \mathfrak{a}P \subseteq \mathfrak{b}P$$

$$P \subseteq Q \implies \mathfrak{a}P \subseteq \mathfrak{a}Q$$

(v) Going to residues modulo P is compatible with inducing modules by ideals, that is given $P \leq_{\mathsf{m}} M$ and $\mathfrak{a} \trianglelefteq_{\mathsf{i}} R$ we get the following equality of sub-modules of M/P

$$\mathfrak{a}\left(M\Big/_P\right) = P + \mathfrak{a}M\Big/_P$$

(vi) The quotient module $M/\mathfrak{a}M$ becomes a well-defined $(R/\mathfrak{a})$-module under the following operations: For any $a \in R$ and $x, y \in M$ we let

$$\begin{aligned}(x + \mathfrak{a}M) + (y + \mathfrak{a}M) &:= (x + y) + \mathfrak{a}M\\ (a + \mathfrak{a})(x + \mathfrak{a}M) &:= (ax) + \mathfrak{a}M\end{aligned}$$

(vii) $(\diamondsuit)$ If M and N are R-modules and $\varphi : M \to N$ is an homomorphism of R-modules, then we obtain a well-defined homomorphism of $(R/\mathfrak{a})$-modules, by letting

$$\varphi\Big/_{\mathfrak{a}} : M\Big/_{\mathfrak{a}M} \to N\Big/_{\mathfrak{a}N} : x + \mathfrak{a}M \mapsto \varphi(x) + \mathfrak{a}N$$

If φ is surjective or bijective, then so is the induced homomorphism $\varphi/\mathfrak{a}$. That is if $\star$ abbreviates any of the words *surjective* or *bijective* then we obtain the implication

$$\varphi \text{ is } \star \implies \varphi\Big/_{\mathfrak{a}} \text{ is } \star$$

Nota $\varphi/\mathfrak{a}$ not necessarily inherits the injectivity of φ. E.g. consider $R = \mathbb{Z}$ and $\mathfrak{a} = 3\mathbb{Z}$. Then $\mathbb{Z} \to \mathbb{Q} : k \mapsto k$ clearly is injective, but $\mathfrak{a}\mathbb{Q} = \mathbb{Q}$ such that $\mathbb{Q}/\mathfrak{a}\mathbb{Q} = 0$ and hence the induced map $\mathbb{Z}/\mathfrak{a}\mathbb{Z} \to \mathbb{Q}/\mathfrak{a}\mathbb{Q}$ cannot be injective.

(viii) Thereby the linear hull of any subset $Z \subseteq M/\mathfrak{a}M$ of the quotient module does not depend on whether we take R or $R/\mathfrak{a}$ as a base ring, that is

$$\mathsf{Lh}_R(Z) = \mathsf{Lh}_{R/\mathfrak{a}}(Z)$$

(ix) Hence a subset $Q \subseteq M/\mathfrak{a}M$ of the quotient module is an R-sub-module of $M/\mathfrak{a}M$ iff it is an $(R/\mathfrak{a})$-sub-module of $M/\mathfrak{a}M$. Therefore the $(R/\mathfrak{a})$-sub-modules of $M/\mathfrak{a}M$ are given to be

$$\mathsf{Subm}_{R/\mathfrak{a}}\left(M\Big/_{\mathfrak{a}M}\right) = \left\{ P\Big/_{\mathfrak{a}M} \;\middle|\; P \leq_{\mathsf{m}} M,\ \mathfrak{a}M \subseteq P \right\}$$

(x) $(\diamondsuit)$ If $\mathfrak{a}, \mathfrak{b} \trianglelefteq_{\mathsf{i}} R$ are ideals of R such that $\mathfrak{a} \subseteq \mathfrak{b}$, then we also get $\mathfrak{a}M \subseteq \mathfrak{b}M$ and thereby the third isomorphism theorem of modules grants the following isomorphy of R-modules

$$M\Big/_{\mathfrak{b}M} \xrightarrow{\sim} M/\mathfrak{a}M\Big/_{\mathfrak{b}M/\mathfrak{a}M} : x + \mathfrak{b}M \mapsto (x + \mathfrak{b}M) + \mathfrak{b}M\Big/_{\mathfrak{a}M}$$

(3.41) Example: (viz. 878)
Let $(R,+,\cdot)$ be a commutative ring and fix any ideal $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$. Then for any non-empty set I, the induced sub-module $\mathfrak{a}R^{\oplus I}$ is nothing but the direct sum $\mathfrak{a}^{\oplus I}$ of I copies of $\mathfrak{a}$

$$\mathfrak{a}R^{\oplus I} \;=\; \mathfrak{a}^{\oplus I}$$

And thereby we obtain an isomorphy of the $(R/\mathfrak{a})$-modules $R^{\oplus I}/\mathfrak{a}R^{\oplus I}$ and $(R/\mathfrak{a})^{\oplus I}$ which can be given explictly, to be the following

$$\left(R \Big/ \mathfrak{a}\right)^{\oplus I} \xrightarrow{\sim} R^{\oplus I} \Big/ \mathfrak{a}R^{\oplus I} \;:\; (b_i + \mathfrak{a}) \mapsto (b_i) + \mathfrak{a}R^{\oplus I}$$

(3.42) Example:
Consider an R-module M a scalar $t \in R$ and sub-modules $P, Q \leq_{\mathfrak{m}} M$. It might be tempting to think that $tQ \subseteq P \subseteq Q$ might yield $P = Q$ - under some reasonable assumptions - as this clearly is true, if R is a skew-field. However this is *not* the case: Instead we find that

$$4\,\mathbb{Z}^2 \;\subset\; \mathbb{Z}\begin{pmatrix}1\\3\end{pmatrix} + \mathbb{Z}\begin{pmatrix}3\\1\end{pmatrix} \;\subset\; \mathbb{Z}^2$$

So here R is a PID (the next best thing after a field), $\mathbb{Z}^2$ is a free, finitely generated module and the generators of P are primitive - refer to (5.26) for a definition. So even in this case $P = Q$ is untrue.

Prob Let us abbreviate $Q := \mathbb{Z}^2$ and $P := \mathbb{Z}(1,3) + \mathbb{Z}(3,1)$. As $(1,3)+(3,1) = (4,4)$ we have $4Q \subseteq P$. But $P \neq Q$, as $(1,0) \notin P$. To see this assume $a(1,3) + b(3,1) = (1,0)$. This would mean $a + 3b = 1$ and $3a + b = 0$. Subtracting the 2nd from the 1st equation we find $-2a + 2b = 1$ which is $2(b-a) = 1$. This would mean $2 \mid 1$ which is untrue.

(3.43) Proposition: (viz. 815)
Let $(R,+,\cdot)$ be a commutative ring and $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$ be an ideal of R. We regard the polynomial ring $R[t]$ as an R-module, as well. Then we get the following properties:

(i) Let $\mathfrak{a}R[t]$ be sub-module of $R[t]$ induced by $\mathfrak{a}$ [note that this is the same, as the push out of the ideal $\mathfrak{a}$ to $R[t]$ in the sense of (8.12)]. Then we find the identity

$$\mathfrak{a}R[t] \;=\; \mathfrak{a}[t] \;:=\; \{\, f \in R[t] \mid \forall\, k \in \mathbb{N} : f[k] \in \mathfrak{a} \,\}$$

(ii) Let us also denote $\widetilde{\mathfrak{a}} := \mathfrak{a}[t] + tR[t] = \{\, f \in R[t] \mid f(0) \in \mathfrak{a} \,\}$, then we obtain two isomorphisms of rings, of the following forms

$$R[t] \Big/ \mathfrak{a}[t] \xrightarrow{\sim} \left(R \Big/ \mathfrak{a}\right)[t] \;:\; f + \mathfrak{a}[t] \mapsto \sum_{k=0}^{\infty} (f[k] + \mathfrak{a})\, t^k$$
$$R[t] \Big/ \widetilde{\mathfrak{a}} \xrightarrow{\sim} R \Big/ \mathfrak{a} \;:\; f + \widetilde{\mathfrak{a}} \mapsto f(0) + \mathfrak{a}$$

(iii) If $\mathfrak{p} \trianglelefteq_{\mathfrak{i}} R$ is a prime ideal, then $\mathfrak{p}[t] \trianglelefteq_{\mathfrak{i}} R[t]$ is a prime ideal, as well. And if $\mathfrak{m} \trianglelefteq_{\mathfrak{i}} R$ is a maximal ideal, then $\widetilde{\mathfrak{m}} \trianglelefteq_{\mathfrak{i}} R[t]$ is a maximal ideal, as well.

(3.44) Lemma: (viz. 968) ($\diamondsuit$)
Let $(R, +, \cdot)$ be a commutative ring, $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be an ideal and consider an R-module M. Then the following statements are true:

(i) If M is a free R-module, with basis $\{ m_i \mid i \in I \}$, then the quotient module $M/\mathfrak{a}M$ is a free $(R/\mathfrak{a})$-module having the basis

$$\{ m_i + \mathfrak{a}M \mid i \in I,\ m_i \notin \mathfrak{a}M \}$$

And thereby the elements of this basis are pairwise distinct. To be precise: If the m_i are pairwise distinct (i.e. for any j, $j \in I$ we get $m_i = m_j \implies i = j$) then the $m_i + \mathfrak{a}M$ are pairwise distinct too, for any i, $j \in I$ with m_i and $m_j \notin \mathfrak{a}M$ we get

$$m_i + \mathfrak{a}M = m_j + \mathfrak{a}M \quad \Longrightarrow \quad i = j$$

(ii) *Lemma of Nakayama:* Given any ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ of R the following two statements are equivalent:

(a) $\mathfrak{a} \subseteq \operatorname{JAC}(R)$

(b) For any finitely generated R-module M we get $\mathfrak{a}M = M \implies M = 0$

(iii) If $P \leq_{\mathrm{m}} M$ is a sub-module of M, such that the quotient module M/P is finitely generated, and $\mathfrak{a} \subseteq \operatorname{JAC}(R)$, then we obtain the implication:

$$M = P + \mathfrak{a}M \quad \Longrightarrow \quad P = M$$

(iv) If N is another R-module, and $\varphi : M \to N$ is an R-module-homomorphism, such that $N/\operatorname{im}(\varphi)$ is finitely generated. If again $\mathfrak{a} \subseteq \operatorname{JAC}(R)$, then we get the following equivalence

$$\varphi \text{ is surjective} \quad \Longleftrightarrow \quad \varphi\big/_{\mathfrak{a}} \text{ is surjective}$$

(v) If M is finitely generated, $\varphi : M \to M$ even is an R-module-endomorphism, and again $\mathfrak{a} \subseteq \operatorname{JAC}(R)$, then we get the following equivalence

$$\varphi \text{ is bijective} \quad \Longleftrightarrow \quad \varphi\big/_{\mathfrak{a}} \text{ is bijective}$$

(vi) *Lemma of Dedekind:* If M is a finitely generated R-module, such that $\mathfrak{a}M = M$, then the ideal $\mathfrak{a}$ contains some element $a \in \mathfrak{a}$ such that $1 - a$ annihilates M. That is

$$(1 - a)M \ = \ 0$$

(3.45) Proposition: (viz. 994)
Let $(R,+,\cdot)$ be a commutative ring and consider an R-module M. Then we obtain the following statements

(i) Suppose that M is finitely generated, that is there are some elements $x_1,\ldots,x_n \in M$ such that $M = \mathrm{Lh}_R\{\, x_1,\ldots,x_n \,\}$. If $\mathfrak{m}M = 0$ for any maximal ideal $\mathfrak{m} \trianglelefteq_{\mathfrak{i}} R$, then M already has to be the zero-module. Formally that is the implication

$$\forall\, \mathfrak{m} \in \mathrm{Smax}(R) : M = \mathfrak{m}M \quad\Longrightarrow\quad M = 0$$

(ii) Suppose $P \leq_{\mathfrak{m}} M$ is a *cofinite* module, that is there are some elements $x_1,\ldots,x_n \in M$ such that $M = P + \mathrm{Lh}_R\{\, x_1,\ldots,x_n \,\}$. Then we get the implication

$$\forall\, \mathfrak{m} \in \mathrm{Smax}(R) : M = P + \mathfrak{m}M \quad\Longrightarrow\quad P = M$$

(iii) If N is another R-module and $\varphi : M \to N$ is an R-module-homomorphism such that $\mathrm{im}(\varphi) \leq_{\mathfrak{m}} N$ is cofinite (i.e. $M = \mathrm{im}(\varphi) + \mathrm{Lh}_R\{\, x_1,\ldots,x_n \,\}$ for some $x_1,\ldots,x_n \in M$). Then we get the equivalence

$$\varphi \text{ is surjective} \quad\Longleftrightarrow\quad \forall\, \mathfrak{m} \in \mathrm{Smax}(R) \;:\; \varphi\big/_{\mathfrak{m}} \text{ is surjective}$$

(iv) If M is finitely generated and $\varphi : M \to M$ is an R-module-endomorphism of M, then we get the following equivalence of

$$\varphi \text{ is bijective} \quad\Longleftrightarrow\quad \forall\, \mathfrak{m} \in \mathrm{Smax}(R) \;:\; \varphi\big/_{\mathfrak{m}} \text{ is bijective}$$

A special case of the above are principal ideals $\mathfrak{a} = tR$, i.e. ideals that are generated by a single element $t \in R$ only. In this case it is clear, that $\mathfrak{a}M = tM := \{\, tx \mid x \in M \,\}$. In other words tM is the image of the endomorphism $x \mapsto tx$ of M. Its kernel will be denoted by M_t and in this sense tM and M_t are two sides of the same coin. Let us take a closer look at this particular coin:

(3.46) Proposition: (viz. 765)
Let $(R,+,\cdot)$ be a commutative ring and fix an element $t \in R$. Let M be an R-module and consider the scalar multiplication by t from the left

$$\mu_t \;:\; M \to M \;:\; x \mapsto tx$$

Let us denote $M_t := \mathrm{kn}(\mu_t) = \{\, x \in M \mid tx = 0 \,\}$ the sub-module of elements of M that are annihilated by t. Then we obtain the following statements:

(i) M_t becomes an (R/tR)-module under its own addition and the well-defined scalar multiplication

$$(a + tR)x \;:=\; ax$$

(ii) If we denote $tM := \mathrm{im}(\mu_t) = \{\, tx \mid x \in M \,\}$, then tM is a sub-module of M, as well, and we obtain the following isomorphy of R-modules

$$M \Big/ M_t \xrightarrow{\sim} tM \,:\, x + M_t \mapsto tx$$

(iii) If M and N are R-modules and $\varphi : M \to N$ is a homomorphism of R-modules, then we have the inclusion of sets: $\varphi(M_t) \subseteq N_t$. And if φ is bijective then we even get the equality $\varphi(M_t) = N_t$.

(iv) If $P_i \leq_{\mathsf{m}} M$ is a family (where $i \in I$) of sub-modules of M, such that M is the inner direct sum of the P_i, then M_t also is the inner direct sum of the sub-modules $(P_i)_t \leq_{\mathsf{m}} M_t$, formally

$$M = \bigoplus_{i \in I} P_i \quad \Longrightarrow \quad M_t = \bigoplus_{i \in I} (P_i)_t$$

(v) $(\diamondsuit)$ Consider some $a_i \in R$ for any $i \in I$ (where I is any non-empty index set), let $b_i := ta_i$ for some fixed $t \in R$ and suppose we have a homomorphism of the form

$$\varphi \,:\, \bigoplus_{i \in I} R \Big/ b_i R \,\to\, M$$

Then there also is the following, well-defined homomorphism $t\varphi$. If φ is surjective and I is finite, then $t\varphi$ is surjective. And if φ is injective and $t \in \mathrm{NZD}(R)$ is a non-zero-divisor, then $t\varphi$ is injective

$$t\varphi \,:\, \bigoplus_{i \in I} R \Big/ a_i R \,\to\, tM \,:\, \Big(r_i + a_i R\Big) \,\mapsto\, \varphi\Big(tr_i + b_i R\Big)$$

(vi) Consider r, s and $t \in R$ such that $t = rs$ and regard the quotient ring $Q := R/tR$ as an R-module. Let $Q_s := \{\, q \in Q \mid sq = 0 \,\}$ again, then we obtain a well-defined homomorphism of R-modules via

$$R \Big/ sR \to \Big(R \Big/ tR\Big)_s \,:\, a + sR \mapsto ra + tR$$

And if $t \in \mathrm{NZD}(R)$ is a non-zero-divisor, this homomorphism already is an isomorphism of R-modules.

(vii) If s, $t \in R$ are any elements of R, as in (vi) we regard $Q := R/tR$ as an R-module and its sub-module $Q_s := \{\, q \in Q \mid sq = 0 \,\}$. Then we find $Q_s = Q$ if and only if t divides s. Formally

$$\Big(R \Big/ tR\Big)_s = R \Big/ tR \quad \Longleftrightarrow \quad t \mid s$$

(viii) If t, $p \in \mathrm{NZD}(R)$ are non-zero-divisors of R, such that p also is a prime element of R, then we obtain the following equivalence (the implication " $\Longleftarrow$ " remains true for arbitrary elements $t \in R$)

$$\Big(R \Big/ tR\Big)_p = 0 \quad \Longleftrightarrow \quad p \not| \, t$$

3.5 Block Decompositions

Algebras - being modules - can often be decomposed into direct sums of sub-modules. However they also carry a multiplicative structure, so the question arises how these two structures interact with one and another. It will turn out, that certain elements of algebras even provide a decomposition by multiplication. This analysis will then be used to study the structure of a group G by studying the structure of the group algebra $F[G]$. This method will be called *representation theory*, so we are about to establish some parts of the machinery for this theory here.

(3.47) Definition:
Let $(R, +, \cdot)$ be an arbitrary ring, M be an R-module and A be an R-algebra. Then we define the following notions for R, M and A respectively:

(i) M is said to be a **simple** R-module if the only sub-modules of M are the trivial ones (0 and M). Formally M is simple, iff the following implication holds true

$$P \leq_{\mathfrak{m}} M \implies P = 0 \text{ or } P = M$$

(ii) M is said to be an **indecomposable** R-module if it does not admit a decomposition as an inner direct sum into non-trivial sub-modules. Formally M is indecomposable iff for any two sub-modules $P, Q \leq_{\mathfrak{m}} M$ the following implication holds true

$$M = P \oplus Q \implies P = 0 \text{ or } Q = 0$$

(iii) M is said to be **completely reducible** if there are some sub-modules $M_i \leq_{\mathfrak{m}} M$ (where $i \in I$) such that all the M_i are simple R-modules and M can be decomposed as the inner direct sum

$$M = \bigoplus_{i \in I} M_i$$

(iv) R is said to be a **simple** ring, if the only ideals of R are the trivial ones (0 and R). Formally R is simple, iff the following implication holds true

$$\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R \implies \mathfrak{a} = 0 \text{ or } \mathfrak{a} = R$$

(v) R is said to be an **indecomposable** ring if it does not admit a decomposition (as an inner direct sum of R-modules) into non-trivial ideals. Formally R is indecomposable iff for any two ideals $\mathfrak{a}$, $\mathfrak{b} \trianglelefteq_{\mathfrak{i}} R$ the following implication holds true

$$R \cong_{\mathfrak{m}} \mathfrak{a} \oplus \mathfrak{b} \implies \mathfrak{a} = 0 \text{ or } \mathfrak{b} = 0$$

(vi) A is said to be a **simple** R-algebra, if the only algebra-ideals of A are the trivial ones (0 and A), Formally A is simple, iff the following implication holds true

$$\mathfrak{a} \trianglelefteq_{\mathfrak{a}} A \implies \mathfrak{a} = 0 \text{ or } \mathfrak{a} = A$$

(vii) A is said to be an **indecomposable** R-algebra if it does not admit a decomposition (as an inner direct sum of R-algebras) into non-trivial, unital sub-algebras. Formally A is indecomposable iff for any two unital subalgebras $U, V \leq_{\mathfrak{b}} A$ the following implication holds true

$$A \cong_{\mathfrak{a}} U \oplus V \implies U = 0 \text{ or } V = 0$$

(ix) A is said to be **completely reducible** if there are some sub-semi-algebras $U_i \leq_{\mathfrak{b}} A$ (where $i \in I$) such that all the U_i are unital and simple R-algebras and A is isomorphic to the exterior direct product of these U_i. That is, iff

$$A \cong_{\mathfrak{a}} \prod_{i \in I} U_i$$

(3.48) Remark:

- If R is commutative then any sub-module $\mathfrak{a} \leq_{\mathfrak{m}} R$ already is an ideal $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$. Hence a commutative ring R is a simple R-module if and only if it is simple as a ring. And likewise a commutative ring R is indecomposable as a ring if and only if it is indecomposable as an R-module.
- Recall that a sub-semialgebra $U \subseteq A$ is said to be *unital* if there is some $e \in U$ such that for any $f \in U$ we get $ef = f = fe$. That is U is an R-algebra with unit element e. If now $U_i \leq_{\mathfrak{b}} A$ is a family of unital sub-semi-algebras, where U_i has the unit element e_i, then $\prod_i U_i$ is an R-algebra with unit element (e_i). Note that this (e_i) is *not* contained in $\oplus_i U_i$ unless I is finite. But in this case the direct product $\prod_i U_i$ and sum $\oplus_i U_i$ are just the same, anyway.

(3.49) Proposition: (viz. 996)
Let $(R, +, \cdot)$ be any non-zero ring $R \neq 0$ and consider two R-modules M and N. Also let $x, y \in M$ be any non-zero elements $x, y \neq 0$. Then we get

(i) M is a simple R-module if and only if all non-zero elements of M already generate M as an R-module. Formally the latter property reads as

$$\forall\, x \in M \,:\, x \neq 0 \implies M = Rx$$

(ii) If $M = Rm$ is a *cyclic* R-module, i.e. it is generated by some element $m \in M$, then M is simple, if and only if $\operatorname{ann}(m) \leq_{\mathfrak{m}} R$ is a maximal R-sub-module of R, that is iff

$$\operatorname{ann}(m) \neq R \quad \text{and} \quad \forall\, P \leq_{\mathfrak{m}} R : \operatorname{ann}(m) \subseteq P \implies \operatorname{ann}(m) = P$$

(iii) If R is a commutative ring and M is a simple R-module, then for any two non-zero elements $0 \neq x, y \in R$ share the same annihilator and this is a maximal ideal of R

$$\operatorname{ann}(x) = \operatorname{ann}(y) \in \operatorname{Smax}(R)$$

(iv) If R is a commutative ring, M is a simple R-module and $0 \neq x, y \in M$ are any two non-zero elements of M, then there is an R-module-automorphism $\Phi : M \xrightarrow{\sim} M$ such that $\Phi(x) = y$

$$\exists\, \Phi \in \mathrm{maut}(M) \;:\; \Phi(x) = y$$

(v) *Lemma of Schur I:* If both M and N are simple R-modules, then any non-zero R-module-homomorphisms form M to N has to be an isomorphism. Formally that is

$$\forall\, \varphi \in \mathrm{mhom}(M,N) \;:\; \varphi \neq 0 \quad\Longrightarrow\quad \varphi \text{ is bijective}$$

(vi) *Lemma of Schur II:* If M is a simple R-module, then the ring $\mathrm{mend}(M)$ of R-module-endomorphism already is a division ring (under composition as multiplication). In particular we get

$$\mathrm{mend}(M) \;=\; \mathrm{maut}(M) \cup \{0\}$$

(vii) If R is a commutative ring, M is a simple R-module and $\varphi : M \to M$ is an R-module-endomorphism, then there is some $a \in R$ such that φ is given to be $\varphi(x) = ax$ (for any $x \in M$).

(3.50) Definition:
Let $(R, +, \cdot)$ be an arbitrary ring and A be an R-semi-algebra. Further consider any three elements x, y and $z \in A$, then we define the following relations on A

$$\begin{aligned} x \perp y \quad &:\Longleftrightarrow \quad xy = 0 \text{ and } yx = 0 \\ z = x \oplus y \quad &:\Longleftrightarrow \quad (x \perp y) \text{ and } z = x + y \end{aligned}$$

Also recall that the **center** $\mathrm{CEN}(A)$ of A is the set of all elements of A, that commute with all others. And $e \in A$ is said to be an **idempotent** of A iff $e^2 = e$. A **central idempotent** thereby is an element $e \in A$ that commutes with all other elements and is an idempotent. That is we define

$$\begin{aligned} \mathrm{CEN}(A) &:= \{\, x \in A \mid \forall\, y \in A : xy = yx \,\} \\ \mathrm{IP}(A) &:= \{\, e \in A \mid e^2 = e \,\} \\ \mathrm{CIP}(A) &:= \mathrm{CEN}(A) \cap \mathrm{IP}(A) \\ \mathrm{SIP}(A) &:= \{\, s \in \mathrm{CIP}(A) \mid s \text{ is simple} \,\} \end{aligned}$$

Thereby an element $s \in A$ is said to be **simple** iff it is a central idempotent such that for any two central idempotents e, $f \in \mathrm{CIP}(A)$ we get the implication

$$s = e \oplus f \quad\Longrightarrow\quad e = 0 \text{ or } f = 0$$

Finally a subset $B \subseteq A$ is said to be a **block** of A if there is some $s \in A$ such that (1) s is simple and (2) B is of the form $B = As = \{\, xs \mid x \in A \,\}$.

(3.51) Proposition: (viz. 998)
Let $(R,+,\cdot)$ be an arbitrary ring and let $A \neq 0$ be a non-zero R-algebra. Then we obtain the properties:

(i) If $B = Ae \subseteq A$ for some central idempotent $e \in \mathrm{CIP}(A)$, we find that B already is (a) an R-sub-semi-algebra $B \leq_{\mathrm{b}} A$ of the A-algebra A, (b) an ideal $B \trianglelefteq_{\mathrm{i}} A$ of the semi-ring A and (c) an R-algebra with unit element $1_B = e$.

(ii) Suppose A is an R-algebra, that is it contains a unit element and thereby even is a ring. Then $\mathrm{CEN}(A) \leq_{\mathrm{a}} A$ is an R-subalgebra and multiplicatively closed subset of A.

(iii) If A is an R-algebra again and $e \in A$ is a (central) idempotent, then $1-e \in A$ is a (central) idempotent as well and we get $e \perp (1-e)$.

(3.52) Proposition: (viz. 998)
Let $(R,+,\cdot)$ be an arbitrary ring and $A \neq 0$ be a non-zero R-algebra, then we obtain the properties:

(i) Suppose the elements $e_1,\ldots,e_n \in A$ have the following properties: (1) $e_1+\cdots+e_n = 1$, (2) $e_i^2 = e_i$ for all $i \in 1\ldots n$ and (3) $e_ie_j = 0$ for all $i \neq j \in 1\ldots n$. Then any $x \in A$ can be written as $x = xe_1+\cdots+xe_n$ and hence A can be decomposed as an inner direct sum of A-sub-modules

$$A \;=\; \bigoplus_{i=1}^{n} Ae_i$$

(ii) If $e_1,\ldots,e_n \in \mathrm{CIP}(A)$ even are central idempotents of A such that (1) $e_1+\cdots+e_n = 1$ and (2) $e_ie_j = 0$ for all $i \neq j \in 1\ldots n$ then the above decomposition respects the multiplication. That is

$$P_i \;:\; A \twoheadrightarrow Ae_i \;:\; x \mapsto xe_i$$

is an epimorphism of A-algebras satisfying $P_i^2 = P_i$ and $P_iP_j = 0$ for any $i \neq j \in 1\ldots n$. The image $\mathrm{im}(P_i) = Ae_i$ not only is an A-sub-module of A, but also a ring with unit element e_i. And the kernel of P_i is given to be the following R-sub-algebra of A

$$\mathrm{kn}(P_i) \;=\; \sum_{j\neq i} Ae_j$$

Therefore we obtain an isomorphy of the R-algebras A and the (exterior) direct sum $Ae_1 \oplus \cdots \oplus Ae_n$

$$A \;\xrightarrow{\sim}\; \bigoplus_{i=1}^{n} Ae_i \;:\; x \mapsto (xe_i)$$

(iii) If A is free, as an R-module then the canonical map $R \hookrightarrow A : a \mapsto a1_A$ is injective and there is an R-submdule $A' \leq_{\mathrm{m}} A$ such that A can be decomposed into an inner direct sum of R-sub-modules

$$A \;=\; R1_A \oplus A'$$

(3.53) Example:

(i) If $e \in \text{IP}(A)$ is a central idempotent of A, then by (3.51.(i)) $1-e \in \text{IP}(A)$ is a central idempotent again, with $e \perp (1-e)$. And according to (3.52.(i)) this yields the decomposition

$$A \;=\; Ae \oplus A(1-e)$$

(ii) Consider an arbitrary ring $(R,+,\cdot)$ and the the R-algebra $A := R^n$ under the point-wise operations $(x_i)+(y_i) = (x_i+y_i)$ and $(x_i)\cdot(y_i) = (x_i \cdot y_i)$. Then R^n has the Euclidean basis $e_j := (\delta_{i,j}) \in R^n$ (where $j \in 1 \ldots n$) and these obviously satisfies $e_i e_j = \delta_{i,j} e_j$. Clearly any $x = (x_i) \in R^n$ can be written uniquely as $x = \sum_i x_i e_i$ such that we have the basis decomposition of R^n

$$R^n \;=\; Re_1 \oplus \ldots \cdots \oplus Re_n$$

And this is just the decomposition of (3.52.(i)) again. Note that other bases of R^n need not yield a decomposition, that is compatible with the multiplication of R^n, as this is due to $e_i e_j = \delta_{i,j} e_j$.

(iii) Now let $(R,+,\cdot)$ be a commutative ring and regard the R-algebra $A = \text{mat}_n(R)$. As in (ii) above let $e_j := (\delta_{i,j}) \in R^n$ (where $j \in 1 \ldots n$) be the Euclidean basis of R^n and let $E_j := E_{j,j} = \text{dia}(e_j)$ be the diagonal matrix of e_j. That is

$$E_1 \;=\; \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & & \vdots \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 \end{pmatrix} \quad \text{up to} \quad E_n \;=\; \begin{pmatrix} 0 & \cdots & \cdots & 0 \\ \vdots & \ddots & & \vdots \\ \vdots & & 0 & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

Then we get $E_1 + \cdots + E_n = \mathbb{1}_n$ and $E_i E_j = \delta_{i,j} E_j$ again such that by (3.52.(i)) we find a decomposition of the R-algebra of $(n \times n)$-matrices

$$\text{mat}_n(R) \;=\; \text{mat}_n(R)E_1 \oplus \cdots \oplus \text{mat}_n(R)E_n$$

Thereby for any $(n \times n)$-matrix $X = (x_{i,j}) \in \text{mat}_n(R)$ it is obvious, that XE_j is just the matrix with a copy of the j-th column of X in it, that is

$$XE_1 \;=\; \begin{pmatrix} x_{1,1} & 0 & \cdots & 0 \\ \vdots & \vdots & \ldots & \vdots \\ x_{n,1} & 0 & \cdots & 0 \end{pmatrix} \quad \text{up to} \quad XE_n \;=\; \begin{pmatrix} 0 & \cdots & 0 & x_{1,n} \\ \vdots & \ldots & \vdots & \vdots \\ 0 & \cdots & 0 & x_{n,n} \end{pmatrix}$$

(3.54) Theorem: (viz. 999)
Let $(R, +, \cdot)$ be a commutative ring and $A \neq 0$ be a non-zero R-algebra. Then we obtain the following two lists of equivalences

(i) We obtain the following equivalences for A being indecomposable as an R-module

(a) A is indecomposable as an A-module

(b) If $e, f \in \text{IP}(A)$ are idempotents of A with $e \perp f$ and $e + f = 1$ then we get $e = 0$ or $f = 0$.

(c) $\text{IP}(A) = \{ 0, 1 \}$

(ii) We obtain the following equivalences for A being indecomposable as an R-algebra

(a) A is indecomposable as an R-algebra

(b) $\text{CEN}(A)$ is indecomposable as an R-algebra

(c) A is a block, that is $A = As$ for some simple $s \in A$

(d) $1 \in A$ is a simple element

(e) $\text{CIP}(A) = \{ 0, 1 \}$

3.6 Dependence Relations

In algebra there are two separate notions of dependence: *Linear dependence* and *algebraic dependence*. A subset S of a module is linearly dependent, if we can find a linear equation with elements of S that turns out 0. A subset S of an algebra is algebraically dependent, if we can find a polynomial equation with elements of S that turns out 0.
Linear dependence yields the notion of a *basis* of a module and we will see that the module's structure is determined by its basis. The same is true with algebraic dependence: This yields the notion of a *transcendence basis*, which determines the structure of the algebra.
It is customary to approach these problems directly and hence separately. Yet there is the underlying concept of *dependence*. So we will try a little more abstract approach: First we will introduce the general notion of a *dependence relation*. Then we will prove (among others) that any dependence relation admits a basis. This will be accomplished in this section.
Consequently it suffices to show that linear dependence (over a skew-field) is a dependence relation, respectively that algebraic dependence (over a field) is a dependence relation. This will be discussed in the sections to come. This approach features the advantage that it neatly separates set-theoretic and algebraic concepts, which yields beautiful clarity and pinpoints precisely where the (skew-)field is involved.

(3.55) Definition:
Let M be an arbitrary set. We will regard relations $\vdash$ of between subsets and elements of M. That is relations of the form $\vdash \subseteq \mathcal{P}(M) \times M$. And for any such relation, elements $x \in M$ and subsets S, $T \subseteq M$ we will use the following notations

$$\begin{aligned} S \vdash x &:\iff (S,x) \in \vdash \\ S \nvdash x &:\iff \neg(S \vdash x) \\ \langle S \rangle &:= \{\, x \in M \mid S \vdash x \,\} \\ \mathrm{sub}(M) &:= \{\, \langle S \rangle \mid S \subseteq M \,\} \\ T \vdash S &:\iff S \subseteq \langle T \rangle \\ &\iff \forall\, x \in S : T \vdash x \end{aligned}$$

Now $\vdash$ is said to be a **dependence relation** on M, iff it is of the form $\vdash \subseteq \mathcal{P}(M) \times M$ and for any elements x, $y \in M$ and subsets S, $T \subseteq M$ it satisfies the following four properties:

(D1) Any element x of S already depends on S, formally this can be put as

$$x \in S \implies S \vdash x$$

(D2) If x depends on S and S depends on T, then x already depends on T

$$T \vdash S,\ S \vdash x \implies T \vdash x$$

(D3) If x depends on S, then it already depends on a finite subset S_x of S

$$S \vdash x \implies \exists\, S_x \subseteq S \,:\, \#S_x < \infty \text{ and } S_x \vdash x$$

(D4) If x depends on S, but not on $S \setminus \{ s \}$ (for some $s \in S$), then we can replace s by x in S, to find a dependency of s on the modified set, formally that is the implication

$$S \vdash x, \text{ and } S \setminus \{ s \} \nvdash x \implies \Big((S \setminus \{ s \}) \cup \{ x \} \Big) \vdash s$$

Equivalently this can be put in the following, technically easier (but a little less intuitive), form: If y depends on $S \cup x$, but not on S alone, then x depends on $S \cup \{ y \}$

$$S \cup \{ x \} \vdash y, \text{ and } S \nvdash y \implies S \cup \{ y \} \vdash x$$

And in case that $\vdash$ is a dependence relation on M we further introduce the following notions: A subset $S \subseteq M$ is said to be **independent** (or more precisely $\vdash$*independent*), iff it satisfies

$$\forall s \in S \ : \ S \setminus \{ s \} \nvdash s$$

Clearly S is said to be **dependent** (or more precisely $\vdash$*dependent*), iff it is not independent (that is $S \setminus \{ s \} \vdash s$ for some $s \in S$). And a subset $B \subseteq M$ is said to be a **basis** (or more precisely a $\vdash$*basis*) iff it is independent and generates M. Formally B is a basis, iff it satisfies

(B1) B is independent

(B2) and $\langle B \rangle = M$

(3.56) Remark:
Let M be any set, such that $\vdash$ is a dependence relation on M and $P \subseteq M$ be any subset of M. Then clearly P inherits this dependence relation: That is for any subset $S \subseteq P$ and any $x \in P$ the relation $S \vdash x$ is a dependence relation again (between the subsets and elements of P).

Prob By construction the restricted relation $S \vdash_P x$ is defined by $S \subseteq P$ and $x \in P$ and $S \vdash x$. As $S \vdash x$ satisfies (D1) to (D4) for *any* $S \subseteq M$ and $x \in M$ these property are in particular satisfied, for those subsets $S \subseteq M$ with $S \subseteq P$ and those elements $x \in M$ with $x \in P$.

(3.57) Lemma: (viz. 866)
Let M be an arbitrary set, $S, T \subseteq M$ be arbitrary subsets and $\vdash$ be a dependence relation on M. Then we obtain all of the following statements

(i) The generation of subsets under $\vdash$ preserves the inclusion of sets, i.e.

$$S \subseteq T \implies \langle S \rangle \subseteq \langle T \rangle$$

(ii) Recall that we denoted $\mathrm{sub}(M)$ to be the set of all $\langle T \rangle$ for some subset $T \subseteq M$. Then for any subset $S \subseteq M$ we obtain the identities

$$\langle \langle S \rangle \rangle = \langle S \rangle = \bigcap \{ P \in \mathrm{sub}(M) \mid S \subseteq P \}$$

(iii) For any subset $S \subseteq M$ the following three statements are equivalent

(a) S is $\vdash$dependent

(b) $\forall\, T \subseteq M : S \subseteq T \implies T$ is $\vdash$dependent

(c) $\exists\, S_0 \subseteq S$ such that $\#S_0 < \infty$ and S_0 is $\vdash$dependent

(iv) For any subset $T \subseteq M$ the following three statements are equivalent

(a) T is $\vdash$independent

(b) $\forall\, S \subseteq M : S \subseteq T \implies S$ is $\vdash$independent

(c) $\forall\, T_0 \subseteq T$ we get $\#T_0 < \infty \implies T_0$ is $\vdash$independent

(v) For any $S \subseteq M$ and $x \in M$ the following statements are equivalent

(a) S is $\vdash$independent and $S \nvdash x$

(b) $S \cup \{ x \}$ is $\vdash$independent and $x \notin S$

(vi) Let $S_i \subseteq M$ be a chain (where $i \in I$) of $\vdash$idependent subsets of M, then the union of the S_i is $\vdash$independent again. Formally that is the implication

$$\left.\begin{array}{lcl} \forall\, i \in I & : & S_i \text{ is } \vdash\text{independent} \\ \forall\, i, j \in I & : & S_i \subseteq S_j \text{ or } S_j \subseteq S_i \end{array}\right\} \implies \bigcup_{i \in I} S_i \text{ is } \vdash\text{independent}$$

(vii) Let $S \subseteq M$ be an $\vdash$independent subset and $T \subseteq M$ be a subset, that generates M, i.e. $M = \langle T \rangle$. If now $S \subseteq T$, then there is a basis B in between S and T. Formally there is some $B \subseteq X$ with

(1) $S \subseteq B \subseteq T$ and

(2) B is a $\vdash$basis of M

(viii) Let $B \subseteq M$ be a $\vdash$basis of M, $b \in B$ and $x \in M$ be arbitrary. Then we denote the set B with b replaced by x by $B' := (B \setminus \{ b \}) \cup \{ x \}$. Then we find the implication

$$B' \vdash b \quad \implies \quad B' \text{ is a } \vdash\text{basis of } M$$

(ix) A subset $B \subseteq M$ is a $\vdash$basis of M if and only if it is a minimal $\vdash$generating subset of M. And this again is equivalent to being a maximal $\vdash$independent subset. Formally that is the equivalence of

(a) B is a $\vdash$basis of M

(b) B generates M (that is $M = \langle B \rangle$) and for any $S \subseteq M$ we obtain

$$S \subset B \quad \implies \quad M \neq \langle S \rangle$$

(c) B is $\vdash$independent and for any $S \subseteq M$ we obtain the implication

$$B \subset S \quad \implies \quad S \text{ is not } \vdash\text{independent}$$

(x) *Basis Exchange Theorem:* Let $B \subseteq M$ be a basis of M and consider an arbitrary subset $A \subseteq B$. Also let $A' \subseteq M$ be a set of elements, satisfying (1) A' is $\vdash$independent and (2) A' generates $\langle A' \rangle = \langle A \rangle$ the same subset, as A. Then we also find

$$\big(B \setminus A\big) \cup A' \text{ is a basis of } M$$

(xi) All $\vdash$bases of M have the same number of elements, formally that is

$$A, B \subseteq M \vdash \text{bases of } M \implies |A| = |B|$$

(xii) If $S \subseteq M$ is $\vdash$independent and $B \subseteq M$ is an $\vdash$basis of M, then S contains no more elements than B, that is $|S| \leq |B|$. Likewise, if $T \subseteq M$ generates $M = \langle T \rangle$, then T contains at least as many elements as B, that is $|B| \leq |T|$.

(xiii) Consider an $\vdash$independent subset $S \subseteq M$ and a $\vdash$basis $B \subseteq M$ of M. Further assume that $\#B < \infty$ is finite, then the following two statements are equivalent

(a) $|S| = |B|$

(b) S is an $\vdash$basis of M

Nota that in the proof of this lemma we did not always require all the properties of a dependence relation. Namely (i), (ii), (iii), (iv), the implication (a) $\implies$ (b) in (v), (vi) and the equivalence (a) $\iff$ (b) in (ix) require the relation $\vdash$ to satisfy properties (D1), (D2) and (D3) only.

(3.58) Remark:
In item (vii) we may chose $S = \emptyset$, as this always is $\vdash$independent respectively $T = M$, as always $M = \langle M \rangle$. These special choices yield the so called *basis selection* respectively *basis completion theorems* (the converse implications follow immediately from (i) and (ii) respectively). And as these are used frequently let us append them here. Thus suppose M is an arbitrary set and $\vdash$ is a dependence relation on M again. Then we get

- *Basis Selection Theorem*: a subset $T \subseteq M$ contains a $\vdash$basis of M if and only if it generates M, that is equivalent are

 (a) $\langle T \rangle = M$

 (b) $\exists\, B \subseteq T \,:\, B$ is a $\vdash$basis of M

- *Basis Completion Theorem*: a subset $S \subseteq M$ can be extended to a $\vdash$basis of M if and only if S is $\vdash$independent, that is equivalent are

 (a) S is $\vdash$independent

 (b) $\exists\, B \subseteq M \,:\, S \subseteq B$ and B is a $\vdash$basis of M

3.7 Linear Dependence

The primary task of any algebraic theory is to classify the objects involved. The same is true for module theory: What types of modules do exist? Surprisingly the answer will strongly depend on the module's base ring. A first complete answer can be given in the case that the base ring is a skew-field S, then all modules over S are of the form $S^{\oplus I}$ for some index set I. (We will later also find complete answers in case the base ring is a PID or DKD. But this is how far the theory carries).
In order to achieve this result we will have to define the notion of a *basis* of a module. Modules with basis will be said to be *free*. However most of the work is done already - all we have to do is prove that *linear dependence* truly is a *dependence relation*, as we have introduced it in the section before.

(3.59) Definition:
Let $(R,+,\cdot)$ be an arbitrary ring an M be R-module. Further consider an arbitrary subset $X \subseteq M$. Then we introduce the following notions

(i) A subset $X \subseteq M$ is said to **generate M as an R-module** (or simply to **R-generate M**), iff the R-module generated by X is M. Formally that is iff (where we also recalled proposition (3.12))

$$M \;=\; \langle X\rangle_{\mathsf{m}} \;=\; \left\{ \sum_{i=1}^{n} a_i x_i \;\middle|\; 1 \leq n \in \mathbb{N},\ a_i \in R,\ x_i \in X \right\}$$

Now X is said to ba a **minimal** R-generating set, iff X R-generates M but any proper subset of X does not R-generate M. Formally X is a minimal R-generating set, iff

$$\forall\, W \subseteq M \;:\; W \subset X \implies \langle W\rangle_{\mathsf{m}} \neq M$$

(ii) We thereby define the **rank** - denoted by $\operatorname{rank}(M)$ - to be the minimal cardinality of any R-generating subset X of M there is. Formally that is

$$\operatorname{rank}(M) \;:=\; \min\{\, |X| \mid X \subseteq M,\ \langle X\rangle_{\mathsf{m}} = M \,\}$$

Nota that this is well defined, as the cardinal numbers are well-ordered - that is any non-empty set of cardinal numbers has a minimal element. Also the defining set above is non-empty, as $M \subseteq M$ and $M = \langle M\rangle_{\mathsf{m}}$. In particular we have $\operatorname{rank}(M) \leq |M|$. Hence this definition yields the following properties: If $I = \operatorname{rank}(M)$ then we get

(1) there is some $X = \{\, x_i \mid i \in I \,\} \subseteq M$ such that $M = \langle X\rangle_{\mathsf{m}}$, and

(2) for any $Y \subseteq M$ with $M = \langle Y\rangle_{\mathsf{m}}$ there is some injective map $\iota : I \hookrightarrow Y$ from I into Y.

(iii) M is said to be **finitely generated**, iff it is R-generated by some finite subset $X \subseteq M$. That is iff M satisfies one of the two following equivalent conditions

(a) $\operatorname{rank}(M) < \infty$

(b) $\exists\, X \subseteq M : \#X < \infty$ and $M = \langle X\rangle_{\mathsf{m}}$

(iv) A sub-module $P \leq_{\mathsf{m}} M$ is said to be **cofinite** (in M), iff you only need to add finitely many to generate M. Formally P is cofinite, iff it satisfies one of the following two equivalent conditions

(a) M/P is finitely generated

(b) $\exists\, X \subseteq M : \#X < \infty$ and $M = P + \langle X \rangle_{\mathsf{m}}$

Nota if $X = \{ x_1, \ldots, x_n \}$ such that $M = P + \langle X \rangle_{\mathsf{m}}$, then it is clear that M/P is generated by the set $\{ x_i + P \mid i \in 1 \ldots n \}$. Vice versa, if $\{ x_i + P \mid i \in 1 \ldots n \}$ generates M/P, then we get $M = P + \langle X \rangle_{\mathsf{m}}$, by taking $X = \{ x_1, \ldots, x_n \}$. Let us prove this: Given any $x \in M$ there are $a_i \in R$ such that $x + P = a_1 x_1 + \cdots + a_n x_n + P$ and hence $x = p + a_1 x_1 + \cdots + a_n x_n \in P + \langle X \rangle_{\mathsf{m}}$ for some $p \in P$.

(v) Let us now introduce a relation of the form $\vdash \subseteq \mathcal{P}(M) \times M$ called the relation of R-**linear dependence**. For any subset $X \subseteq M$ and any element $x \in M$ let us define

$$X \vdash x \quad :\Longleftrightarrow \quad \begin{array}{l} \exists\, n \in \mathbb{N}, \exists\, x_1, \ldots, x_n \in X, \exists\, a_1, \ldots, a_n \in R \\ \text{such that } x = a_1 x_1 + \cdots + a_n x_n \end{array}$$

Nota that we allowed $n = 0$ in this definition. And by convention the empty sum is set to be 0. Thus we get $X \vdash 0$ for any subset $X \subseteq M$. In fact we even get $\emptyset \vdash x \iff x = 0$ for any $x \in M$.

(vi) A subset $X \subseteq M$ is said to be R-**linearly dependent** iff for any $1 \leq n \in \mathbb{N}$, any $\{ x_1, \ldots, x_n \} \subseteq X$ and any $a_1, \ldots, a_n \in R$ we get

$$\left.\begin{array}{l} a_1 x_1 + \cdots + a_n x_n = 0 \\ \forall\, i, j \in 1 \ldots n : x_i = x_j \implies i = j \end{array}\right\} \implies \quad a_1 = \cdots = a_n = 0$$

If this is not the case (i.e. there are some $a_1, \ldots, a_n \in R \setminus \{0\}$ and pairwise distinct $x_1, \ldots, x_n \in X$ such that $a_1 x_1 + \cdots + a_n x_n = 0$), then X is said to be R-**linearly dependent**. Finally X is said to be a **maximal** R-linearly independent set, iff X is R-linearly dependent, but any proper superset of X is R-linearly dependent. Formally

$$\forall\, Y \subseteq M \;:\; X \subset Y \implies Y \text{ is } R\text{-linearly dependent}$$

(vii) A subset $B \subseteq M$ is said to be a R-**basis** of M, iff it is R-linearly independent (that is (vi)) and R-generates M (that is (i)). And M is said to be **free**, iff it has a basis. That is

$$M \text{ free} \quad \Longleftrightarrow \quad \exists\, B \subseteq M \;:\; B \text{ is a } R\text{-basis}$$

(viii) Finally an ordered tupel $(x_i) \subseteq M$ (where $i \in I$) is said to be an **ordered** R-**basis** of M, iff it satisfies the following two properties

(1) $\{ x_i \mid i \in I \}$ is a R-basis of M

(2) $\forall\, i, j \in I \;:\; x_i = x_j \implies i = j$

(3.60) Example: (viz. 870)

(i) A very special case in the above definitions is the zero-module $0 = \{0\}$. It is a free module, as $\emptyset \subseteq \{0\}$ is an R-basis of 0. And thereby for an arbitrary R-module M we obtain

$$\mathrm{rank}(M) = 0 \quad \Longleftrightarrow \quad M = \{0\}$$

(ii) From the above definitions it is clear, that M is finitely generated, if and only if the zero-sub-module $0 \leq_{\mathfrak{m}} M$ is cofinite (in M). Also, if P and $Q \leq_{\mathfrak{m}} M$ are sub-modules of M such that P is cofinite and $P \subseteq Q$, then Q is cofinite as well.

(iii) Consider an integral domain $(R, +, \cdot)$ and an R-sub-module (that is an ideal) $\mathfrak{a} \leq_{\mathfrak{m}} R$. Then $\mathfrak{a}$ is a free R-module, if and only if it is a principal ideal

$$\mathfrak{a} \text{ free} \quad \Longleftrightarrow \quad \exists\, a \in R \,:\, \mathfrak{a} = aR$$

(iv) The standard example of a free module is the following: Let $(R, +, \cdot)$ be an arbitrary ring and $I \neq \emptyset$ be any non-empty set. Then we consider

$$R^{\oplus I} \;=\; \bigoplus_{i \in I} R \;=\; \left\{ (x_i) \in R^I \;\middle|\; \#\{\, i \in I \mid x_i \neq 0 \,\} < \infty \right\}$$

Recall that this is an R-module under the component-wise operations $(x_i) + (y_i) := (x_i + y_i)$ and $a(x_i) := (ax_i)$ - where a, a_i and $y_i \in R$. For any $j \in I$ let us denote the **j-th Euclidean vector**

$$e_j \;:=\; (\delta_{i,j}) \;\in\; R^{\oplus I}$$

That is e_j contains 1 exactly once, at the j-th position; all other entries are 0. In other words still: The i-th component of e_j is 1 if and only if $i = j$ and 0 otherwise. Then $R^{\oplus I}$ is a free R-module having the so called **Euclidean basis**

$$\mathcal{E} \;=\; \{\, e_j \mid j \in I \,\}$$

($\diamondsuit$) In particular, if R is a commutative ring, or skew-field, we find that for any set $I \neq \emptyset$ the R-module $R^{\oplus I}$ is free and has dimension $|I|$, as $\mathcal{E}$ is an R-basis of $R^{\oplus I}$

$$\dim\left(R^{\oplus I}\right) \;=\; |I|$$

(3.61) Proposition: (viz. 871)
Let $(R, +, \cdot)$ be an arbitrary ring and M be an R-module. Let us denote the relation of R-linear dependence by $\vdash$ again (refer to (3.59.(iv)). Then the following statements hold true

(i) The relation $\vdash$ of R-linear dependence satisfies the properties (D1), (D2) and (D3) of a dependence relation (refer to (3.55) for the explicit definitions), but not necessarily (D4).

(ii) Recall that for a subset $X \subseteq M$ we defined $\langle X \rangle = \{\, y \in M \mid X \vdash y \,\}$, then we obtain the identities

$$\langle X \rangle \;=\; \langle X \rangle_{\mathfrak{m}} \;=\; \mathrm{Lh}_R(X)$$

(iii) For any subset $X \subseteq M$ the following three statements are equivalent

(a) X is $\vdash$dependent

(b) $\forall\, Y \subseteq M : X \subseteq Y \implies Y$ is $\vdash$dependent

(c) $\exists\, X_0 \subseteq X$ such that $\#X_0 < \infty$ and X_0 is $\vdash$dependent

(iv) For any subset $Y \subseteq M$ the following three statements are equivalent

(a) Y is $\vdash$independent

(b) $\forall\, X \subseteq M : X \subseteq Y \implies X$ is $\vdash$independent

(c) $\forall\, Y_0 \subseteq Y$ we get $\#Y_0 < \infty \implies Y_0$ is $\vdash$independent

(v) A subset $B \subseteq M$ is a $\vdash$basis of M if and only if it is a minimal $\vdash$generating subset of M. Formally that is the equivalence of the following two statements

(a) B is a $\vdash$basis of M

(b) $M = \langle B \rangle$ and $S \subset B \implies M \neq \langle S \rangle$

(vi) A subset $B \subseteq M$ is an R-basis of M if and only if any $x \in M$ has a unique representation as an R-linear combination over B. Formally that is the equivalence of the following two statements

(a) B is an R-basis of M

(b) for any element $x \in M$ there is a uniquely determined tupel $(x_b) \in R^{\oplus B}$ such that x can be represented as a linear combination over the $b \in B$, that is

$$x \;=\; \sum_{b \in B} x_b b$$

Nota that the sum occurring in (b) is well-defined, as only finitely many of the x_b are non-zero. Further note that in fact the existence of such a representation is equivalent to $M = \langle B \rangle_{\mathsf{m}}$ and the uniqueness of the representation is equivalent to the R-linear independence of B.

(3.62) Proposition: (viz. 873)
Let $(R, +, \cdot)$ be any ring and M be an R-module with basis $B \subseteq M$. Consider some subset $A \subseteq B$ and let $P := \mathrm{Lh}_R(A)$ be the sub-module of M generated by A only. Then we obtain the following statements

(i) The quotient module M/P is a free module again, we can explicitly a basis of M/P to be the following set: $\{\, b + P \mid b \in B \setminus A \,\}$ is a basis of M/P.

(ii) *Basis Exchange Theorem*: If $A' \subseteq M$ is another set, such that (1) A' is linearly independent and (2) $\mathrm{Lh}_R(A') = P$ generates the same sub-module, as A, then we find another basis of M by

$$\big(B \setminus A\big) \cup A' \;\text{ is a basis of } M$$

(3.63) Proposition: (viz. 874)
Let $(R, +, \cdot)$ be an integral domain and denote $E := \mathrm{QUOT}(R)$ its quotient field. Also let $I \neq \emptyset$ be any non-empty set and $X \subseteq R^{\oplus I}$. Now the embedding $R \hookrightarrow E : a \mapsto a/1$ gives rise to an embedding $R^{\oplus I} \hookrightarrow E^{\oplus I}$ canonically. In this sense we consider $X \subseteq E^{\oplus I}$, as well. Then the following two statements are equivalent

(a) $X \subseteq R^{\oplus I}$ is R-linearly independent

(b) $X \subseteq E^{\oplus I}$ is E-linearly independent

(3.64) Proposition: (viz. 872)
Let $(S, +, \cdot)$ be a skew-field and M be an S-module. Let us denote the relation of S-linear dependence by $\vdash$ again (refer to (3.59.(iv))). Then we obtain the following statements, in addition to (3.61)

(i) The relation $\vdash$ of S-linear dependence satisfies properties (D1) to (D4) and thereby is a dependence relation [refer to (3.55) for the explicit definitions]. In fact $\vdash$ satisfies the following, slightly stronger property (for any $X \subseteq M$ and any $x, y \in M$)

$$X \vdash y,\ x \in X,\ y \neq 0 \quad \Longrightarrow \quad \Big((X \setminus \{ x \}) \cup \{ y \} \Big) \vdash x$$

(ii) Let $X \subseteq M$ be an arbitrary subset, then the following two statements are equivalent (for arbitrary rings we only get (b) $\Longrightarrow$ (a) here)

(a) X is $\vdash$independent

(b) X is S-linearly independent

(iii) For any $X \subseteq M$ and $y \in M$ the following statements are equivalent

(a) $X \cup \{ y \}$ is S-linearly independent and $y \notin X$

(b) X is S-linearly independent and $X \nvdash y$

(iv) For any subset $B \subseteq M$ all of the following statements are equivalent

(a) B is a $\vdash$basis of M

(b) B is an S-basis of M

(c) B is a minimal S-generating subset of M, that is B generates M [i.e. $M = \mathrm{Lh}_S(B)$], but any proper subset $X \subset B$ does not suffice to generate M

$$X \subset B \quad \Longrightarrow \quad M \neq \mathrm{Lh}_S(X)$$

(d) B is a maximal S-linearly independent subset, that is B is S-linearly independent and any subset $X \subseteq M$ strictly containing B no longer is S-linearly independent

$$B \subset X \quad \Longrightarrow \quad X \text{ is not } S\text{-linearly independent}$$

(e) Any element $x \in M$ can be represented as a uniquely determined linear combination over the elements of B. That is for any $x \in M$, there is a uniquely determined $(x_b) \in S^{\oplus B}$ such that

$$x \;=\; \sum_{b \in B} x_b b$$

(v) Let $X \subseteq M$ be a S-linearly independent subset and $Y \subseteq M$ be a generating subset $M = \mathrm{Lh}_S(Y)$. If now $X \subseteq Y$, then there is some $B \subseteq M$ such that

(1) $X \subseteq B \subseteq Y$ and

(2) B is an S-basis of M

(vi) All S-bases of M have the same number of elements, formally that is

$$A, B \subseteq M \; S\text{-bases of } M \quad \Longrightarrow \quad |A| = |B|$$

(3.65) Remark:
By (3.64.(iv)) S-linear dependence is a dependence relation and the notions of *bases* are the same. But due to (3.58) M then already has a basis B or, in other words, M is a free module. That is we have arrived at a crucial, much celebrated result:

Any module M over a skew-field S already is free!

Now by (3.64.(vi)) all S-bases of M share the same cardinality. Hence we may define the **dimension** of M over S to be the cardinality of *any* S-basis of M. That is we let

$$\dim_S(M) \;:=\; |B| \quad \text{where} \quad B \text{ is an } S\text{-base of } M$$

(3.66) Proposition: (viz. 872)
Let $(S, +, \cdot)$ be a skew-field and M be an S-module. Let us denote the relation of S-linear dependence by $\vdash$ again (refer to (3.59.(iv))). Then we obtain the following statements in addition to (3.61) and (3.64)

(vii) A set of S-linearly elements contains at most $\dim_S(M)$ many elements

$$X \subseteq M \text{ is } S\text{-linearly independent} \quad \Longrightarrow \quad |X| \leq \dim_S(M)$$

(viii) Suppose M is finite-dimensional (i.e. $\dim_S(M) < \infty$) and consider an S-linearly independent subset $X \subseteq M$. Then the following two statements are equivalent

(a) $|X| = \dim_S(M)$

(b) X is an S-basis of M

(ix) Im particular if M is finite-dimensional and $P \leq_{\mathrm{m}} M$ is a sub-module of $\dim(P) = \dim(M) < \infty$ equal dimension, then they already are equal $P = M$, themselves.

(3.67) Remark: (viz. 875)
Let us summarize a bit: If $(R,+,\cdot)$ is a ring, M is an R-module and $\mathcal{M} \subseteq M$ is a subset of M. Let us denote the set of functions from $\mathcal{M}$ to R that are non-zero for finitely many $m \in \mathcal{M}$ only, by

$$\mathcal{F}_0(\mathcal{M},R) \;:=\; \{\, a : \mathcal{M} \to R \;\mid\; \#\{\, m \in \mathcal{M} \mid a(m) \neq 0 \,\} \,\}$$

It is clear, that any $a \in \mathcal{F}_0(\mathcal{M},R)$ corresponds to an R-linear combination of the elements of $\mathcal{M}$. That is the following map is well defined

$$\varrho \;:\; \mathcal{F}_0(\mathcal{M},R) \;\to\; M \;:\; a \;\mapsto\; \sum_{m\in\mathcal{M}} a(m)m$$

The image of ϱ is precisely the R-linear hull of $\mathcal{M}$. And from the construction it is clear that we have the following list of equivalences concerning ϱ and M

$$\begin{aligned} \varrho \text{ is injective} &\iff \mathcal{M} \text{ is linearly independent} \\ \varrho \text{ is surjective} &\iff \mathcal{M} \text{ generates } M \\ \varrho \text{ is bijective} &\iff \mathcal{M} \text{ is a basis of } M \end{aligned}$$

If both $\mathcal{M}$ and R are finite, then $\mathcal{F}_0(\mathcal{M},R) = \mathcal{F}(\mathcal{M},R)$ is finite as well, having $(\#R)^{\#\mathcal{M}}$ elements. If $\mathcal{M}$ or R is infinite then the weird rules of cardinal arithmetic set in: In this case, if M is a free R-module, then the cardinality of M is the maximum of the cardinalities of M and one of its bases $\mathcal{M}$

$$|M| \;=\; \max\{\, |R|, \dim(M) \,\}$$

(3.68) Lemma: (viz. 875)
Let $(S,+,\cdot)$ be a skew-field and consider two S-modules V and W. Then we obtain the following formulae concerning their dimensions

(i) If P and $Q \leq_{\mathsf{m}} V$ are any two S-sub-modules of V, then the dimension of the sum $P+Q$ satisfies the following relation

$$\dim(P+Q) \;=\; \dim(P) + \dim(Q) - \dim(P\cap Q)$$

(ii) If $P \leq_{\mathsf{m}} V$ is an S-sub-module of V then the dimension of the quotient is just the difference of the dimensions of V and P

$$\dim\left(V \,\middle/\, P\right) \;=\; \dim(V) - \dim(P)$$

(iii) If $\varphi : V \to W$ is any S-linear map, then we obtain the following *dimension formula* for the dimension of the kernel and image of φ

$$\dim(V) \;=\; \dim\big(\mathrm{kn}(\varphi)\big) + \dim\big(\mathrm{im}(\varphi)\big)$$

3.8 Homomorphisms

Homomorphism of modules - better known as linear maps - are one of the most common concepts of algebra. Examples are abundant: Derivation and integration of functions, both are linear, the arithmetical mean is linear, matrices are just another way to define linear maps, etc. The advantage of linear maps is, that they are both, well-understood and well-behaved. In fact this concept is so successful, that many theories (e.g. chaos theory) thrive on finding linear approximations for non-linear problems.

(3.69) Definition:

(i) Let $(R,+,\cdot)$ be any ring and consider two R-modules M and N. Then a map $\varphi : M \to N$ is said to be an R-**module-homomorphism** or simply an R-**linear** map, iff for any $a \in R$, x, $y \in M$ we get

$$\begin{aligned} \varphi(ax) &= a\varphi(x) \\ \varphi(x+y) &= \varphi(x)+\varphi(y) \end{aligned}$$

We will denote the set of all R-module-homomorphisms from M to N by $\mathrm{mhom}(M,N)$ or, in order to emphasize the base ring R, by $\mathrm{mhom}_R(M,N)$. In linear algebra (i.e. primarily in case of a base field R) it is also customary to simply write $\mathcal{L}(M,N)$:

$$\mathcal{L}(M,N) \;:=\; \{\, \varphi : M \to N \mid \varphi \text{ is an } R\text{-module-homomorphism} \,\}$$

$$\mathrm{mhom}(M,N) \;:=\; \mathrm{mhom}_R(M,N) \;:=\; \mathcal{L}(M,N)$$

(ii) Consider any two rings $(R,+,\cdot)$ and $(S,+,\cdot)$ and fix a homomorphism of rings $\alpha : R \to S$. Then a map $\varphi : M \to N$ is said to be an α-**module-homomorphism** or simply an α-**linear** map, iff for any $a \in R$ and any x, $y \in M$ we get

$$\begin{aligned} \varphi(ax) &= \alpha(a)\varphi(x) \\ \varphi(x+y) &= \varphi(x)+\varphi(y) \end{aligned}$$

We will denote the set of all R-module-homomorphisms from M to N by $\mathrm{mhom}_\alpha(M,N)$ or, in case α is understood, simply by $\mathrm{mhom}(M,N)$. In linear algebra (i.e. primarily in case of a base field R) it is also customary to write $\mathcal{L}_\alpha(M,N)$:

$$\mathcal{L}_\alpha(M,N) \;:=\; \{\, \varphi : M \to N \mid \varphi \text{ is an } \alpha\text{-module-homomorphism} \,\}$$

$$\mathrm{mhom}(M,N) \;:=\; \mathrm{mhom}_\alpha(M,N) \;:=\; \mathcal{L}_\alpha(M,N)$$

(iii) In any case (i) and (ii) we define the **kernel** $\mathrm{kn}(\varphi)$ and the **image** $\mathrm{im}(\varphi)$ of the map $\varphi : M \to N$ to be the following subsets of M or N respectively

$$\begin{aligned} \mathrm{kn}(\varphi) &:= \{\, x \in M \mid \varphi(x) = 0 \,\} &&\subseteq M \\ \mathrm{im}(\varphi) &:= \{\, \varphi(x) \mid x \in M \,\} &&\subseteq N \end{aligned}$$

And we establish the usual nomenclature: φ is said to be a **mono- epi-** or **isomorphism**, iff it is a homomorphism, that also is injective, surjective or bijective respectively:

φ is called	iff φ is
monomorphism	injective
epimorphism	surjective
isomorphism	bijective

(iv) In case (i), an R-module-homomorphism $\varphi : M \to M$ acting solely on the R-module M is called an R-**module-endomorphism**. And it is called an R-**module-automorphism**, iff it also is bijective

φ is called	iff φ is
endomorphism	$M = N$
automorphism	$M = N$ and bijective

(v) If M and N are any two R-modules, then M and N are said to be **isomorphic**, iff there is an isomorphism of R-modules from M to N, formally we write

$$M \cong_{\mathsf{m}} N \quad :\Longleftrightarrow \quad \exists\, \Phi : M \to N \;\; R\text{-module isomorphism}$$

(3.70) Example:

(i) The most easy and completely trivial example is the *zero-homomorphism*. If M and N are any two R-modules, then we obtain an R-module-homomorphism 0 by letting

$$0 \;:\; M \to N \;:\; x \mapsto 0$$

(ii) Another trivial example of an R-module-homomorphism is the *identity map* $\mathbb{1}$ on some R-module M, that simply returns the element x it was given

$$\mathbb{1} \;:\; M \to M \;:\; x \mapsto x$$

(iii) A slight generalization is the map of set theoretical inclusion, which (by abuse of notation) is written as $\subseteq$ again. If $P \leq_{\mathsf{m}} M$ is a sub-module of the R-module M, then we get an R-module-homomorphism by

$$\subseteq \;:\; P \to M \;:\; x \mapsto x$$

(iv) Regard $M := R[t]$ the polynomial ring over R, as an R-module. Then for any $f \in R[t]$ we define the *derivation* of f to be the following polynomial again

$$\partial f(t) \;:=\; \sum_{k=1}^{\infty} k f[k]\, t^{k-1} \;\in\; R[t]$$

And thereby $\partial : R[t] \to R[t]$ is a homomorphism of R-modules, with $\mathrm{im}(\partial) \subseteq R[t]$ and $R \subseteq \mathrm{kn}(\partial)$. In fact we will study such maps more closely in section 7.6 and see, that ∂ is no homomorphism of rings, as it satisfies the property $\partial(f \cdot g) = (\partial f) \cdot g + f \cdot (\partial g)$ for any $f, g \in R$.

(3.71) Remark: (viz. 766)

(i) The notion (ii) of α-linearity clearly includes the case (i) of R-linearity - just take $\alpha = \mathbb{1} : R \to R$, then an α-linear map $\varphi : M \to N$ is nothing but an R-linear map.

(ii) If $\varphi : M \to N$ is an R-module-homomorphism, then the kernel and image of φ are sub-modules of M and N respectively:

$$\begin{aligned} \mathrm{kn}(\varphi) &= \{\, x \in M \mid \varphi(x) = 0 \,\} &\leq_{\mathfrak{m}}\ M \\ \mathrm{im}(\varphi) &= \{\, \varphi(x) \mid x \in M \,\} &\leq_{\mathfrak{m}}\ N \end{aligned}$$

More generally: If $\varphi : M \to N$ is an α-module-homomorphism then $\mathrm{kn}(\varphi)$ is an R-sub-module of M. And if α is surjective, then $\mathrm{im}(\varphi)$ also is an S-sub-module of N.

(iii) If $\varphi : M \to N$ is an R-module-homomorphism, then φ is surjective iff its image is N and φ is injective iff its kernel is 0, formally these are the equivalences

$$\begin{aligned} \varphi \text{ is surjective} &\iff \mathrm{im}(\varphi) = N \\ \varphi \text{ is injective} &\iff \mathrm{kn}(\varphi) = \{0\} \end{aligned}$$

(iv) If R is any ring and M and N are any R-modules, also $P \leq_{\mathfrak{m}} M$ and $Q \leq_{\mathfrak{m}} N$ are sub-modules of M and N respectively and $\varphi : M \to N$ is an R-module-homomorphism, then $\varphi(P) \leq_{\mathfrak{m}} N$ and $\varphi^{-1}(Q) \leq_{\mathfrak{m}} M$ are sub-modules of N and M again:

$$\begin{aligned} \varphi(P) &= \{\, \varphi(x) \mid x \in P \,\} &\leq_{\mathfrak{m}}\ N \\ \varphi^{-1}(Q) &= \{\, x \in M \mid \varphi(x) \in Q \,\} &\leq_{\mathfrak{m}}\ M \end{aligned}$$

More generally: If $\varphi : M \to N$ is an α-module-homomorphism then $\varphi^{-1}(Q)$ is an R-sub-module of M. And if α is surjective, then $\varphi(P)$ also is an S-sub-module of N.

(v) If L, M and N all are R-modules and the maps $\varphi : L \to M$ and $\psi : M \to N$ both are homomorphisms of R-modules then the composition $\psi\varphi$ is a homomorphism of R-modules as well

$$\psi\varphi \ :\ L \to N \ :\ x \mapsto \psi(\varphi(x))$$

More generally: Suppose L is an R-module, M is an S-module and N is an T-module, where $(R, +, \cdot)$, $(S, +, \cdot)$ and $(T, +, \cdot)$ are arbitrary rings. Further we fix ring homomorphisms $\alpha : R \to S$ and $\beta : S \to T$. If now $\varphi : L \to M$ is an α-module-homomorphism and $\psi : M \to N$ is an β-module-homomorphism, then the composition $\psi\varphi : L \to N$ is an $(\beta\alpha)$-module-homomorphism.

(vi) If M and N are R-modules, where $(R,+,\cdot)$ is a commutative ring, then the set $\mathrm{mhom}_R(M,N)$ of all R-module-homomorphisms from M to N becomes an R-module in itself. Thereby for any φ, $\psi \in \mathrm{mhom}_R(M,N)$ and any $a \in R$ we take the following operations

$$\begin{aligned} \varphi+\psi &: M \to N : \quad x \mapsto \varphi(x)+\psi(x) \\ a\varphi &: M \to N : \quad x \mapsto a\varphi(x) \end{aligned}$$

(vii) More generally: Suppose $(R,+,\cdot)$ is an arbitrary and $(S,+,\cdot)$ is a commutative ring, M is an R-module and N is an S-module. Further fix a homomorphism $\alpha : R \to S$ of rings. Then $\mathrm{mhom}_\alpha(M,N)$ becomes an S-module under the above operations of (vi).

(viii) If $(R,+,\cdot)$ is a commutative ring and M is an R-module, then the set $\mathrm{end}(M) = \mathrm{mhom}(M,M)$ of module R-homomorphisms $\varphi : M \to M$ from M to itself is a commutative ring $(\mathrm{end}(M),+,\circ)$ under the point-wise addition $\varphi+\psi : x \mapsto \varphi(x)+\psi(x)$ and composition $\circ$ of maps $\varphi\psi : x \mapsto \varphi(\psi(x))$. The unit element of $\mathrm{end}(M)$ is the identity map $\mathbb{1}_M : x \mapsto x$.

(ix) If $(R,+,\cdot)$ is any ring, M is an R-module, $P \leq_{\mathsf{m}} M$ is a sub-module of M and $\Phi \in \mathrm{maut}(M)$ an automorphism of M, then we obtain the following isomorphy of R-modules

$$M\big/_P \xrightarrow{\sim} M\big/_{\Phi(P)} \; : \; x+P \mapsto \Phi(x)+\Phi(P)$$

(x) Consider any non-empty subset $X \subseteq M$, $X \neq \emptyset$ of M. Then we examine the R-module-homomorphism that takes tuples (a_x) to linear combinations over the elements of X

$$\varrho \; : \; R^{\oplus X} \to M \; : \; (a_x) \mapsto \sum_{x \in X} a_x x$$

Note that ϱ is well-defined, as in any $(a_x) \in R^{\oplus X}$ only finitely many a_x are non-zero. Also - as the compositions on $R^{\oplus X}$ are component-wise - it is clear, that ϱ truly is a homomorphism of R-modules. Yet ϱ also satisfies a number of interesting properties

$$\begin{aligned} \mathrm{im}(\varrho) &= \mathrm{Lh}_R(X) \\ \varrho \text{ is surjective} &\iff X \text{ generates } M \\ \varrho \text{ is injective} &\iff X \text{ is } R\text{-linearly independent} \\ \varrho \text{ is bijective} &\iff X \text{ is an } R\text{-basis of } M \end{aligned}$$

In particular, iff $B \subseteq M$ is a basis, then ϱ is an isomorphy of R-modules $\varrho : R^{\oplus B} \xrightarrow{\sim} M$. That is all free R-modules are of the form $R^{\oplus B}$ for some set B.

(3.72) Proposition: (viz. 768)
Let $(R,+,\cdot)$ be an arbitrary ring and consider any two R-modules M and N. Then we find the statements:

(i) If $X \subseteq M$ generates M, that is $M = \ln(X)$, and $\varphi, \psi : M \to N$ are any two R-linear maps, then the equality of φ and ψ is determined on X. That is the equivalency of

$$\varphi\big|_X \;=\; \psi\big|_X \quad\Longleftrightarrow\quad \varphi \;=\; \psi$$

(ii) And if $B \subseteq M$ even is an R-basis of M and $n : B \to N$ is an arbitrary map from B to N, then there is a uniquely defined R-linear map $\varphi : M \to N$ satisfying $\varphi\big|_B = n$. (It is customary to say that φ is generated by *linear expansion* of the map n). And this is given to be

$$\varphi\left(\sum_{x\in B} a_x x\right) \;:=\; \sum_{x\in B} a_x n(x)$$

(3.73) Definition: (viz. 769)

(i) Fix a commutative ring $(R,+,\cdot)$ and consider the three R-modules L, M and N. If $\psi : M \to N$ is an R-module-homomorphism, then ψ induces another R-module-homomorphism ψ_* called the **push-forward** of ψ by letting

$$\psi_* \;:\; \mathrm{mhom}_R(L,M) \to \mathrm{mhom}_R(L,N) \;:\; \varphi \mapsto \psi\varphi$$

(ii) Fix a commutative ring $(R,+,\cdot)$ and consider the three R-modules L, M and N. If $\varphi : L \to M$ is an R-module-homomorphism, then φ induces another R-module-morphism φ^* called the **pull-back** of φ by letting

$$\varphi^* \;:\; \mathrm{mhom}_R(N,M) \to \mathrm{mhom}_R(L,N) \;:\; \psi \mapsto \psi\varphi$$

(iii) More generally: Suppose L is an R-module, M is an S-module and N is a T-module, where $(R,+,\cdot)$ is an arbitrary, $(S,+,\cdot)$ and $(T,+,\cdot)$ are commutative rings. Further we fix ring homomorphisms $\alpha : R \to S$ and $\beta : S \to T$. If now $\psi : M \to N$ is an β-module-homomorphism, then ψ induces another $\beta\alpha$-module-homomorphism ψ_* called the **push-forward** of ψ by letting

$$\psi_* \;:\; \mathrm{mhom}_\alpha(L,M) \to \mathrm{mhom}_{\beta\alpha}(L,N) \;:\; \varphi \mapsto \psi\varphi$$

(iv) Suppose L is an R-module, M is an S-module and N is a T-module, where $(R,+,\cdot)$ is an arbitrary, $(S,+,\cdot)$ and $(T,+,\cdot)$ are commutative rings. Further we fix ring homomorphisms $\alpha : R \to S$ and $\beta : S \to T$. If now $\psi : M \to N$ is an β-module-homomorphism, then φ induces another $\beta\alpha$-module-homomorphism φ^* called the **bf pull-back** of φ by letting

$$\varphi^* \;:\; \mathrm{mhom}_\beta(M,N) \to \mathrm{mhom}_{\beta\alpha}(L,N) \;:\; \psi \mapsto \psi\varphi$$

(3.74) Proposition: (viz. 769)
Let M be an R-module over an arbitrary ring $(R,+,\cdot)$ and consider $\pi : M \to M$ an R-module-endomorphism. We say that π is a *projection* if $\pi^2 = \pi$ and in this case the image of π is given to be $\mathrm{im}(\pi) = \{\, x \in M \mid \pi(x) = x \,\}$ and thereby M is the inner direct product of

$$M \;=\; \mathrm{im}(\pi) \oplus \mathrm{kn}(\pi)$$

We have introduced *linear* maps, that is homomorphisms of modules. And we have also introduced products of modules. Sometimes we will want to consider maps on products of modules, that respect the module structure on every single module. These maps will be called *multilinear*, but as the general definition might be somewhat irritating, let us regard the easiest yet most important case beforehand:
Let $(R,+,\cdot)$ be a ring and consider three R-modules M_1, M_2 and N. Then a map $\varphi : M_1 \times M_2 \to N$ is said to be **bilinear** (sometimes they are called *balanced* instead) if for any $a \in R$, any $x_1, y_1 \in M_1$ and any $x_2, y_2 \in M$ it satisfies the following four properties:

$$\begin{aligned}
\varphi(ax_1, x_2) &= a\,\varphi(x_1, x_2) \\
\varphi(x_1 + y_1, x_2) &= \varphi(x_1, x_2) + \varphi(y_1, x_2) \\
\varphi(x_1, ax_2) &= a\,\varphi(x_1, x_2) \\
\varphi(x_1, x_2 + y_2) &= \varphi(x_1, x_2) + \varphi(x_1, y_2)
\end{aligned}$$

In other words φ is *linear in the first argument* [i.e. for any $x_2 \in M_2$ the map $M_1 \to N : x_1 \mapsto \varphi(x_1, x_2)$ is a homomorphism of R-modules] and *linear in the second argument* [i.e. for any $x_1 \in M_1$ the map $M_2 \to N : x_1 \mapsto \varphi(x_1, x_2)$ is a homomorphism of R-modules]. This clearly can be generalized to arbitrarily numerous products of modules: What we require of a *multilinear* map is, that is linear in every single of its arguments. This is the easy idea behind the following (a little hard to read) definition. In this sense a bilinear map is nothing more than a multilinear map, where the index is $I = \{\, 1, 2 \,\}$.

(3.75) Definition:
Let $(R,+,\cdot)$ be any ring and consider a family (M_i) (where $i \in I$ and $I \neq \emptyset$) of R-modules. Let finally M be a sub-module of the exterior direct product

$$M \;\leq_{\mathrm{m}}\; \prod_{i \in I} M_i$$

(i) Let N be another R-module, then a map $\varphi : M \to N$ is said to be **R-multilinear**, iff for any $i \in I$ and any fixed $(x_j)_{j \neq i}$ [where $x_j \in M_j$ for $i \neq j \in I$] the map $M_i \to N : x_i \mapsto \varphi(x)$ [where $x = (x_j)_{j \in I}$] is R-linear. That is for any $i \in I$ let us abbreviate arbitrary elements of the M_j for $j \neq i$ by dots, then for any $a \in R$ and any $x_i, y_i \in M_i$ we require φ to satisfy

$$\begin{aligned}
\varphi(\ldots, ax_i, \ldots) &= a\varphi(\ldots, x_i, \ldots) \\
\varphi(\ldots, x_i + y_i, \ldots) &= \varphi(\ldots, x_i, \ldots) + \varphi(\ldots, y_i, \ldots)
\end{aligned}$$

(ii) Let $(S,+,\cdot)$ be another ring, let N be an S-module and fix a ring-homomorphism $\alpha : R \to S$. Then a map $\varphi : M \to N$ is said to be **α-multilinear**, iff for any $i \in I$ and any fixed $(x_j)_{j\neq i}$ [where $x_j \in M_j$ for $i \neq j \in I$] the map $M_i \to N : x_i \mapsto \varphi(x)$ [where $x = (x_j)_{j\in I}$] is α-linear. That is for any $i \in I$ let us abbreviate arbitrary elements of the M_j for $j \neq i$ by dots, then for any $a \in R$ and any x_i, $y_i \in M_i$ we require φ to satisfy

$$\begin{aligned} \varphi(\dots, ax_i, \dots) &= \alpha(a)\varphi(\dots, x_i, \dots) \\ \varphi(\dots, x_i + y_i, \dots) &= \varphi(\dots, x_i, \dots) + \varphi(\dots, y_i, \dots) \end{aligned}$$

(3.76) Example: (viz. 769)
Let $(R,+,\cdot)$ be any ring, then we can simultaneously regard $R^2 = R \oplus R$ as an R-module or as a product of two R-modules R. In particular we can consider both R-linear and R-bilinear maps:

(i) The addition map $\alpha : R^2 \to R : (a,b) \mapsto a+b$ on R is R-linear but *not* necessarily R-bilinear.

(ii) The multiplication map $\mu : R^2 \to R : (a,b) \mapsto ab$ is R-bilinear but *not* necessarily R-linear.

(iii) The canonical projections $\pi_1 : R^2 \to R : (a,b) \mapsto a$ and $\pi_2 : R^2 \to R : (a,b) \mapsto b$ are R-linear but *not* necessarily R-bilinear.

(iv) If $(R,+,\cdot)$ is an arbitrary ring and M is an R-module, then the properties of being an R-module precisely state, that the scalar multiplication of M is R-bilinear

$$R \times M \to M \ : \ (a,x) \mapsto ax$$

(v) ($\diamondsuit$) If $(R,+,\cdot)$ is a *commutative* ring and $1 \leq \ell$, m and $n \in \mathbb{N}$ then the multiplication of matrices is R-bilinear, as well. Thereby the multiplication is a map of the following form

$$\mathrm{mat}_{\ell,m}(R) \times \mathrm{mat}_{m,n}(R) \to \mathrm{mat}_{\ell,n}(R) \ : \ (A,B) \mapsto AB$$

(vi) ($\diamondsuit$) The complex numbers $\mathbb{C}$ have the complex conjugation κ as a field-automorphism which is defined to be $\kappa(x+iy) = x - iy$. This is usually denoted by $\overline{z} = \kappa(z)$ for $z = x+iy \in \mathbb{C}$. If now U and V are $\mathbb{C}$-vectorspaces, then a map $\varphi : U \times V \to \mathbb{C}$ is said to be *sesqui-linear*, iff it satisfies the following four properties:

$$\begin{aligned} \varphi(au, v) &= a\,\varphi(u,v) \\ \varphi(u+u', v) &= \varphi(u,v) + \varphi(u',v) \\ \varphi(u, av) &= \overline{a}\,\varphi(u,v) \\ \varphi(u, v+v') &= \varphi(u,v) + \varphi(u,v') \end{aligned}$$

for any $a \in \mathbb{C}$, u, $u' \in U$ and v, $v' \in V$. That is φ is $\mathbb{C}$-linear in the first argument, but a κ-homomorphism in the second argument. We will study and use such maps in section 4.7.

3.9 Isomorphism Theorems

In this section we will study several basic properties of homomorphisms of R-modules. First of all we will encounter the fundamental "isomorphism theorems". Later on we will get some more advanced criteria whether an endomorphism is an isomorphism. A more general way to look at homomorphisms is to study chains of homomorphisms. This is the ascent of homological algebra and we will already introduce the fundamental concepts and its first properties here.

(3.77) Proposition: (viz. 770)
Let $(R,+,\cdot)$ be any ring and consider a homomorphism $\Phi : M \to N$ between the R-modules M and N. Then the following statements are equivalent (and in this case we already get $\alpha = \beta = \Psi = \Phi^{-1}$)

(a) Φ is bijective

(b) There is some homomorphism $\Psi : N \to M$ of R-modules, such that $\Psi\Phi = \mathbb{1}_M$ and $\Phi\Psi = \mathbb{1}_N$

(c) There are arbitrary maps $\alpha : N \to M$ and $\beta : N \to M$, such that $\alpha\Phi = \mathbb{1}_M$ and $\Phi\beta = \mathbb{1}_N$

(3.78) Theorem: (viz. 770)
Let $(R,+,\cdot)$ be any ring and consider any two R-modules M and N. Let further $\varphi : M \to N$ be an R-module-homomorphism, then the following statements are true

(i) If $P \leq_{\mathfrak{m}} M$ and $Q \leq_{\mathfrak{m}} N$ are sub-modules of M and N respectively, such that $P \subseteq \varphi^{-1}(Q)$, then we obtain a well-defined homomorphism of R-modules, by letting

$$\overline{\varphi} : M\big/_P \to N\big/_Q : x+P \mapsto \varphi(x)+Q$$

(ii) **1st Isomorphism Theorem:** Any R-module-homomorphism $\varphi : M \to N$ induces an isomorphism of R-modules from the quotient module $M/\mathrm{kn}(\varphi)$ to $\mathrm{im}(\varphi)$ by virtue of

$$\overline{\varphi} : M\big/_{\mathrm{kn}(\varphi)} \xrightarrow{\sim} \mathrm{im}(\varphi) : x+\mathrm{kn}(\varphi) \mapsto \varphi(x)$$

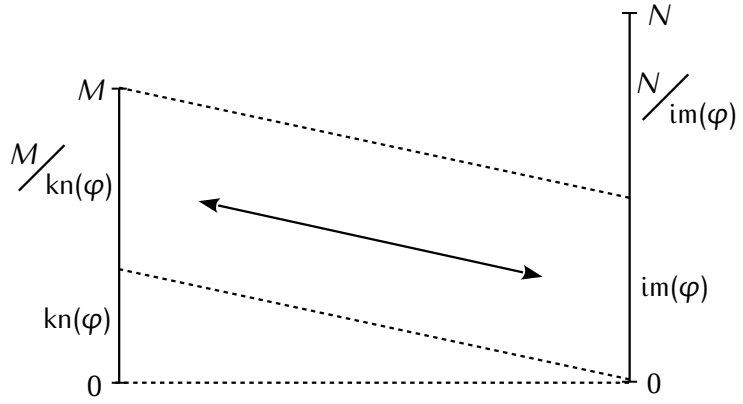
(iii) **2nd Isomorphism Theorem:** If P and $Q \leq_{\mathfrak{m}} M$ are any two sub-modules of M, we obtain another isomorphism of R-modules, by virtue of

$$Q\big/_{P\cap Q} \xrightarrow{\sim} P+Q\big/_P : x+P\cap Q \mapsto x+P$$

(iv) **3rd Isomorphism Theorem:** If P and $Q \leq_{\mathfrak{m}} M$ are sub-modules of M again, such that $P \subseteq Q$, then we obtain one more isomorphism of R-modules, by virtue of

$$M\big/_Q \xrightarrow{\sim} M/P\big/_{Q/P} : x+Q \mapsto (x+P)+Q\big/_P$$

(3.79) Remark:
The following illustration should help to foster an intuitive understanding of what the first isomorphism theorem is all about: We see M on the left-hand side and N on the right hand side. The kernel of φ is the part of M that is mapped to 0 in N. The "rest" $M/\mathrm{kn}(\varphi)$ is copied - without loss of structure or information - to $\mathrm{im}(\varphi)$ which is part of N. The "rest" $N/\mathrm{im}(\varphi)$ of N is of unknown size and structure.



(3.80) Proposition: (viz. 771)
Consider the module M over an arbitrary ring $(R,+,\cdot)$ and let $P \leq_{\mathsf{m}} M$ be a sub-module of M. Then the following statements are equivalent

(a) There is an isomorphism Φ of the form given below, that also satisfies $\Phi(P) = P \oplus 0 = P \times \{\, 0 + P \,\}$

$$\Phi \;:\; M \;\xrightarrow{\sim}\; P \oplus M\big/_P$$

(b) P is a *direct summand* of M, i.e. there is another sub-module $Q \leq_{\mathsf{m}} M$ of M such that $M = P + Q$ and $P \cap Q = 0$, such that M is the inner direct sum

$$M \;=\; P \oplus Q$$

(c) There is a projection $\pi : M \to M$, that is an endomorphism with $\pi^2 = \pi$, such that $\mathrm{im}(\pi) = P$.

(3.81) Remark:
If M is an R-module over some ring $(R,+,\cdot)$ and $P \leq_{\mathsf{m}} M$ is a sub-module such that $M = P \oplus Q$ for some other sub-module $Q \leq_{\mathsf{m}} M$, then the above proposition yields an isomorphism of the form

$$M \;\cong_{\mathsf{m}}\; P \oplus M\big/_P \;:\; p + q \mapsto (p, q + P)$$

However an isomorphism of this form need not exist in general. As a counterexample we consider $M = \mathbb{Z}$ as an $R = \mathbb{Z}$ module with its ideal (i.e. sub-module) $2\mathbb{Z} \leq_{\mathsf{m}} \mathbb{Z}$. The quotient $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$ only consists of the elements $\overline{0} = 0 + 2\mathbb{Z}$ and $\overline{1} = 1 + 2\mathbb{Z}$. Suppose there was some isomorphism $\Phi : \mathbb{Z} \xrightarrow{\sim} 2\mathbb{Z} \oplus \mathbb{Z}_2$. We will disprove this by regarding $c := \Phi^{-1}(0,\overline{1}) \in \mathbb{Z}$. Clearly $\Phi(2c) = 2(0,\overline{1}) = (0,\overline{0})$. But as Φ is injective, this means $2c = 0$. Yet $\mathbb{Z}$ has no zero-divisors such that $c = 0$ in contradiction to $\Phi(c) = (0,\overline{1}) \neq 0$.

(3.82) Corollary: (viz. 971)

(i) Consider a commutative ring $(R,+,\cdot)$ and a finitely generated R-module M. If now $\varphi : M \to M$ is an R-module-endomorphism, then the following two statements are equivalent:

(a) φ is surjective

(b) φ is bijective

(ii) Consider a commutative ring $(R,+,\cdot)$ and an artinian R-module M. If now $\varphi : M \to M$ is an R-module-endomorphism, then the following two statements are equivalent:

(a) φ is injective

(b) φ is bijective

(iii) Consider a skew-field $(S,+,\cdot)$ and a finitely generated S-module V. If now $\varphi : V \to V$ is an S-module-endomorphism, then the following three statements are equivalent:

(a) φ is injective

(b) φ is surjective

(c) φ is bijective

(3.83) Lemma: (viz. 994)
Let $(R,+,\cdot)$ be a commutative ring then the following statements are true

(i) If $R \neq 0$ is non-zero and I, $J \neq \emptyset$ are any two non-empty sets, then $R^{\oplus I}$ is isomorphic (as an R-module) to $R^{\oplus J}$ iff I and J have the same cardinality, formally that is

$$R^{\oplus I} \cong_{\mathfrak{m}} R^{\oplus J} \quad \Longleftrightarrow \quad |I| = |J|$$

(ii) Let $\mathfrak{a}$, $\mathfrak{b} \trianglelefteq_{\mathfrak{i}} R$ be two ideals in R, if now $R/\mathfrak{a}$ and $R/\mathfrak{b}$ are isomorphic as R-modules, then $\mathfrak{a}$ and $\mathfrak{b}$ already have to be equal, as subsets of R

$$R\Big/_{\mathfrak{a}} \cong_{\mathfrak{m}} R\Big/_{\mathfrak{b}} \quad \Longleftrightarrow \quad \mathfrak{a} = \mathfrak{b}$$

(3.84) Remark:

- The statement of (i) need not be true for non-commutative rings R. As an example fix the $\mathbb{Z}$-module $M := \mathbb{Z}^{\oplus\mathbb{N}}$ and take to the ring of $\mathbb{Z}$-module endomorphisms of M

 $$S := \operatorname{end}(M)$$

 Then for any $m, n \in \mathbb{N}$ we find that $S^m \cong_{\mathfrak{m}} S^n$ are isomorphic as S-modules. In fact it suffices to give a basis of S consisting of two elements. It is easy to see $M \cong_{\mathfrak{m}} M \oplus M$ and hence

 $$\begin{aligned} S &= \operatorname{mhom}(M,M) \cong_{\mathfrak{m}} \operatorname{mhom}(M, M\oplus M) \\ &\cong_{\mathfrak{m}} \operatorname{mhom}(M,M) \oplus \operatorname{mhom}(M,M) = S^2 \end{aligned}$$

For more details on this construction refer to [Scheja, Storch, Algebra 1, Kapitel 25 Beispiel 3 and Kapitel 36 Beispiel 2], which is the source of this counter-example.

- A ring R with the property of (i) is also called to have IBN (invariant basis number). Thus (i) may be expressed as *commutative rings have IBN*. Of course there is a multitude of non-commutative rings that have IBN, as well. An important example is: If $\varphi : R \twoheadrightarrow S$ is a ring-epimorphism and S has IBN then R has IBN, as well. For more comments on this, please refer to the first chapter of [Lam, A first Course in non-commutative Rings, GTM 131].

- In (ii) it does not suffice to have an isomorphism of R-modules $\mathfrak{a} \cong_{\mathsf{m}} \mathfrak{b}$. E.g. regard the ring $S := R[s,t]$. If we now define the ideals $\mathfrak{a} := tS$ and $\mathfrak{b} := stS$ then $\mathfrak{a}$ and $\mathfrak{b}$ clearly are isomorphic as R-modules, but

$$\begin{array}{lll} S\big/_{\mathfrak{a}} & \cong_{\mathsf{a}} & R[s] \\ S\big/_{\mathfrak{b}} & \cong_{\mathsf{a}} & R[s] \oplus tR[t] \end{array}$$

- In (3.99.(ii)) we will present a much stronger statement: If M is a free R-module, then any R-basis of M has cardinality $\mathsf{rank}(M)$ - supposed R is commutative. And as the isomorphism $R^{\oplus I} \cong_{\mathsf{m}} R^{\oplus J}$ transfers bases we could conclude

$$|I| \;=\; \mathsf{rank}(R^{\oplus I}) \;=\; \mathsf{rank}(R^{\oplus J}) \;=\; |J|$$

 Yet the proof of this statement is far longer and uses substantially more tools (the theory of noetherian modules), hence we have chosen to give a more direct proof in advance.

(3.85) Definition:
Fix any number $1 \leq n \in \mathbb{N}$ and a ring $(R, +, \cdot)$. Further consider some R-modules M_i (where $i \in 0 \dots n$) and some R-module-homomorphisms, $\varphi_i : M_{i-1} \to M_i$ (where $i \in 1 \dots n$). That is we have

(1) for any $i \in 0 \dots n$: M_i is an R-module

(2) for any $i \in 1 \dots n$: $\varphi_i : M_{i-1} \to M_i$ is an R-module homomorphism

Let us denote $M = (M_i)$ and $\varphi = (\varphi_i)$, then the ordered pair (M, φ) is said to be a **(finite) chain** of R-modules. And in this case we will use a rather intuitive notation for the chain (M, φ), namely

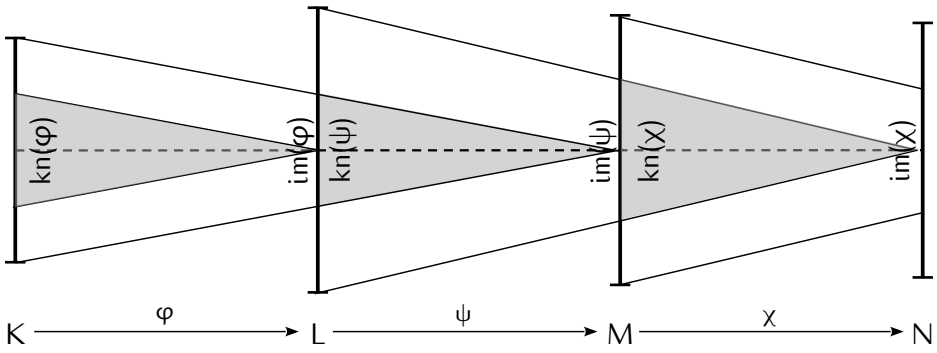
$$M_0 \xrightarrow{\varphi_1} M_1 \xrightarrow{\varphi_2} M_2 \to \cdots \to M_{n-1} \xrightarrow{\varphi_n} M_n$$

And a chain (M, φ) is said to be a **complex** of R-modules, iff we also have the following property (C). Nota an equivalent formulation of (C) is: $\varphi_i \varphi_{i-1} = 0$ for any $i \in 2 \dots n$. And (M, φ) is said to be an **exact chain** of R-modules, iff apart from (1) and (2) it also satisfies the even stronger property (E), where

(C) for any $i \in 2 \dots n$ we have $\mathsf{im}(\varphi_{i-1}) \subseteq \mathsf{kn}(\varphi_i)$

(E) for any $i \in 2 \dots n$ we have $\mathsf{im}(\varphi_{i-1}) = \mathsf{kn}(\varphi_i)$

(3.86) Remark:
The following diagram is supposed to help illustrating the concept of an exact chain in an example featuring 4 modules K, L, M and N. The fact that the image of the previous homomorphism is exactly the kernel of the subsequent homomorphism turns into the condition, that the connecting lines from one module (e.g. from K) to 0 in the over-next module (in M) goes straight and does not leave a gap:



(3.87) Remark:

(i) If $M_i = 0$, then we necessarily have $\varphi_i = 0$ and $\varphi_{i+1} = 0$, that is $\varphi_i : M_{i-1} \to 0 : x_{i-1} \mapsto 0$ and $\varphi_{i+1} : 0 \to M_{i+1} : 0 \mapsto 0$. As these maps are already determined, we don't have to denote them in the chain of modules and may just write

$$M_{i-2} \xrightarrow{\varphi_{i-1}} M_{i-1} \to 0 \to M_{i+1} \xrightarrow{\varphi_{i+2}} M_{i+2}$$

If this chain is exact, then it even follows that $\ker(\varphi_{i+2}) = 0$ and $\operatorname{im}(\varphi_{i-1}) = M_{i-1}$ such that φ_{i+2} is injective and φ_{i-1} is surjective, formally these are the implications

$$\begin{aligned} M_i = 0 \quad &\Longrightarrow \quad \varphi_{i+2} \text{ is injective} \\ M_i = 0 \quad &\Longrightarrow \quad \varphi_{i-1} \text{ is surjective} \end{aligned}$$

Prob due to the exactness of the chain we get $\operatorname{im}(\varphi_{i-1}) = \ker(\varphi_i) = \ker(0) = M_{i-1}$ and hence φ_{i-1} is surjective. Likewise $\ker(\varphi_{i+2}) = \operatorname{im}(\varphi_{i+1}) = \operatorname{im}(0) = 0$ and hence φ_{i+2} is injective.

(ii) In particular for any R-module homomorphism $\varphi : M \to N$ we get a chain of R-modules, by taking

$$0 \to M \xrightarrow{\varphi} N \to 0$$

And this chain is exact if and only if φ is an isomorphism. Prob due to (i) the chain is exact, iff φ is injective and surjective, that is iff φ is bijective. And that's when φ is called an isomorphism.

(iii) In a similar fashion we find a chain-version of the first isomorphism theorem: Given an exact chain (i.e. $\operatorname{im}(\psi) = N$ and $\ker(\psi) = \operatorname{im}(\varphi)$) of R-modules, of the form

$$L \xrightarrow{\varphi} M \xrightarrow{\psi} N \to 0$$

the first isomorphism theorem of R-modules yields the following isomorphism, induced by ψ

$$M\Big/_{\mathrm{im}(\varphi)} \xrightarrow{\sim} N \,:\, x+\mathrm{im}(\varphi) \mapsto \psi(x)$$

(iv) A **short exact sequence** of R-modules is an exact chain of R-modules ($n=5$) of the following form:

$$0 \to L \xrightarrow{\varphi} M \xrightarrow{\psi} N \to 0$$

And as we have seen (iii) this induces an isomorphism $M/\mathrm{im}(\varphi) \xrightarrow{\sim} N$. But as in this case φ also is injective, we have $\varphi : L \xrightarrow{\sim} L' := \mathrm{im}(\varphi)$, that is there is an isomorphic copy $L' \leq_{\mathfrak{m}} M$ of L in M. And for this we get $M/L' \xrightarrow{\sim} N$, according to (iii). This is the essence of what a short exact chain of R-modules is about.

(3.88) Example:

(i) Any sub-module $P \leq_{\mathfrak{m}} M$ gives rise to a canonical short exact sequence, by taking the inclusion $\subseteq : x \mapsto x$ and the canonical projection $\varrho(x) := x + P$

$$0 \to P \xrightarrow{\subseteq} M \xrightarrow{\varrho} M\Big/_P \to 0$$

(ii) Any R-module-homomorphism $\varphi : M \to N$ induces a canonical short exact sequence of R-modules

$$0 \to \mathrm{kn}(\varphi) \xrightarrow{\subseteq} M \xrightarrow{\varphi} \mathrm{im}(\varphi) \to 0$$

(iii) But φ also induces another chain of R-modules: Let us denote $\pi : N \to N/\mathrm{im}(\varphi) : y \mapsto y + \mathrm{im}(\varphi)$ the canonical projection, then we find another exact chain of R-modules, by taking

$$0 \to \mathrm{kn}(\varphi) \xrightarrow{\subseteq} M \xrightarrow{\varphi} N \xrightarrow{\pi} N\Big/_{\mathrm{im}(\varphi)} \to 0$$

(iv) Another, most important example is the following: Consider any two R-modules L and N. Let us denote the canonical embedding of L into $L \oplus N$ by $\iota : L \to L \oplus N : x \mapsto (x,0)$ and the canonical projection onto N by $\pi : L \oplus N \to N : (x,y) \mapsto y$. Then $\mathrm{im}(\iota) = L \oplus 0 = \mathrm{kn}(\pi)$, such that we get the short exact chain of R-modules

$$0 \to L \xrightarrow{\iota} L \oplus N \xrightarrow{\pi} N \to 0$$

(v) Let us alter the above example a little: Given two sub-modules P and $Q \leq_{\mathfrak{m}} M$ of some R-module M, we take the maps $\sigma : P \cap Q \to P \oplus Q : x \mapsto (x,x)$ and $\delta : P \oplus Q \to P + Q : (x,y) \mapsto x - y$. Then we get an exact chain of R-modules

$$0 \to P \cap Q \xrightarrow{\sigma} P \oplus Q \xrightarrow{\delta} P + Q \to 0$$

Passing to quotients we find another exact chain of R-modules: This time the homomorphisms are given to be $\sigma : x \mapsto (x+P, x+Q)$ and $\delta : (x+P, y+Q) \mapsto (x-y) + (P+Q)$

$$0 \to M\big/_{P\cap Q} \xrightarrow{\sigma} M\big/_{P} \oplus M\big/_{Q} \xrightarrow{\delta} M\big/_{P+Q} \to 0$$

We see that in the first chain $\delta : P \oplus Q \xrightarrow{\sim} P + Q$ is an isomorphism iff $P \cap Q = 0$ and in the second chain $\sigma : M/(P \cap Q) \xrightarrow{\sim} M/P \oplus M/Q$ is an isomorphism iff $M = P + Q$.

(vi) A special case of (v) is the following: Consider any two distinct prime numbers $2 \leq p \neq q \in \mathbb{Z}$. By the Chinese remainder theorem we get $\mathbb{Z}_p \oplus \mathbb{Z}_q = \mathbb{Z}_{pq}$. Thereby the canonical maps become $\iota : \mathbb{Z}_p \to \mathbb{Z}_{pq} : a + p\mathbb{Z} \mapsto aq + pq\mathbb{Z}$ and $\pi : \mathbb{Z}_{pq} \to \mathbb{Z}_q : b + pq\mathbb{Z} \mapsto b + q\mathbb{Z}$. And hence we obtain the short exact sequence of $\mathbb{Z}$-modules

$$0 \to \mathbb{Z}_p \xrightarrow{\iota} \mathbb{Z}_{pq} \xrightarrow{\pi} \mathbb{Z}_q \to 0$$

(3.89) Lemma: (viz. 842)
Let $(R, +, \cdot)$ be a commutative ring. If the following chain of R-modules is exact [that is φ is injective, ψ is surjective and $\mathrm{im}(\varphi) = \mathrm{kn}(\psi)$] then statements (a), (b) and (c) are equivalent

$$0 \to L \xrightarrow{\varphi} M \xrightarrow{\psi} N \to 0$$

(a) There is some homomorphism $\alpha : M \to L$ such that $\alpha\varphi = \mathbb{1}_L$

(b) There is some homomorphism $\omega : N \to M$ such that $\psi\omega = \mathbb{1}_N$

(c) There is an isomorphism $\Phi : M \xrightarrow{\sim} L \oplus N$ such that the following diagram commutes

$$\begin{array}{ccccccccc} 0 & \to & L & \xrightarrow{\varphi} & M & \xrightarrow{\psi} & N & \to & 0 \\ & & = & & \downarrow \Phi & & = & & \\ 0 & \to & L & \xrightarrow{\iota} & L \oplus N & \xrightarrow{\pi} & N & \to & 0 \end{array}$$

Nota That the above diagram in (c) commutes, is to say $\Phi\varphi = \iota$ and $\pi\Phi = \psi$. And in this case we already have $\mathrm{kn}(\alpha) = \mathrm{im}(\omega)$ and M is the (inner) direct sum of the sub-modules

$$M \;=\; \mathrm{kn}(\alpha) \oplus \mathrm{im}(\varphi) \;=\; \mathrm{im}(\omega) \oplus \mathrm{kn}(\psi)$$

(3.90) Corollary: (viz. 845)
Let $(R, +, \cdot)$ be a commutative ring and assume the following short chain of R-modules is exact:

$$0 \to L \xrightarrow{\varphi} M \xrightarrow{\psi} N \to 0$$

If N is free, then (a), (b) and (c) in (3.89) are true, that is there is an isomorphism $\Phi : M \xrightarrow{\sim} L \oplus N$ such that the following diagram commutes

$$\begin{array}{ccccccccc} 0 & \to & L & \xrightarrow{\varphi} & M & \xrightarrow{\psi} & N & \to & 0 \\ & & = & & \downarrow \Phi & & = & & \\ 0 & \to & L & \xrightarrow{\iota} & L \oplus N & \xrightarrow{\pi} & N & \to & 0 \end{array}$$

(3.91) Remark:
We usually are interested in the isomorphism $\Phi : M \xrightarrow{\sim} L \oplus N$. So let us give the construction of this isomorphism that is used in the proof of lemma (3.89): If α is given, then we can give Φ straight away. If conversely ω is given, then we can explicitly give the inverse Φ^{-1} isomorphism instead:

$$\Phi \ : \ M \ \xrightarrow{\sim} \ L \oplus N \ : \ x \mapsto (\alpha(x), \psi(x))$$

$$\Phi^{-1} \ : \ L \oplus N \ \xrightarrow{\sim} \ M \ : \ (u, p) \mapsto \varphi(u) + \omega(p)$$

In (3.90), if N is free, we get the isomorphism Φ by constructing a suitable map $\omega : N \to M$: Let $\{ n_i \mid i \in I \}$ be a basis of N and for any $i \in I$ choose some $m_i \in M$ such that $\psi(m_i) = n_i$. Then we can define $\omega(\sum_i a_i n_i) := \sum_i a_i m_i$ and thereby get Φ as above.

The next few theorems will be concerned with chains of modules. While this may look a little weird, if this is your first encounter with this notion, it truly is a powerful language, that will be developed further. In fact there is an entire mathematical discipline called *homological algebra* dedicated to studying these objects. And the method of using chains and diagrams is also known as *diagram-chasing*. So let us start with some fundamental properties of chains:

(3.92) Lemma: (viz. 992)
Let $(R, +, \cdot)$ be a ring, $n \geq 2$ and for any $i \in 1 \dots n$ consider $\varphi_i : M_{i-1} \to M_i$ and $\psi_i : N_{i-1} \to N_i$ some R-module homomorphisms. Also suppose, that for any $i \in 0 \dots n$ there is some isomorphism of R-modules $\Phi_i : M_i \xrightarrow{\sim} N_i$ such that we may regard the following diagram

$$\begin{array}{ccccccccc} M_0 & \xrightarrow{\varphi_1} & M_1 & \xrightarrow{\varphi_2} & M_2 & \to \dots & \xrightarrow{\varphi_n} & M_n \\ \updownarrow & & \updownarrow & & \updownarrow & & & \updownarrow \\ N_0 & \xrightarrow{\psi_1} & N_1 & \xrightarrow{\psi_2} & N_2 & \to \dots & \xrightarrow{\psi_n} & N_n \end{array}$$

Suppose this diagram commutes, that is for any $i \in 1 \dots n$ we have $\Phi_i \varphi_i = \psi_i \Phi_{i-1}$. Then the following two statements are equivalent

(a) The chain $M_0 \to M_1 \to M_2 \to \cdots \to M_n$ is exact (resp. a complex)

(b) The chain $N_0 \to N_1 \to N_2 \to \cdots \to N_n$ is exact (resp. a complex)

The following lemma may seem a little strange at a first glance: It studies the effect of pull-back and push-forward of homomorphisms of modules. The right setting in which to formulate this is the new-forged language of chains of modules. Here all the properties take a neat compact form - though the punch of this approach will only later reveal itself, when we regard tensor products of modules.
In the language of homological algebra it could be put as: The push-forward is a left-exact, covariant functor, whereas the pull-back is a left-exact contra-variant functor. But let's not get ahead of ourselves and just focus on one of the staging points of homological algebra:

(3.93) Lemma: (viz. 992)
Let $(R,+,\cdot)$ be a (not necessarily commutative) ring and consider the R-modules U, V, W and M such that the following chain of modules is exact

$$0 \to U \xrightarrow{\varphi} V \xrightarrow{\psi} W$$

Recall the definition of the push-forward $\varphi_* : \mathcal{L}(M,U) \to \mathcal{L}(M,V)$ defined by $\varphi_*(f) = \varphi f$, then the following chain of R-modules is exact, as well

$$0 \to \mathcal{L}(M,U) \xrightarrow{\varphi_*} \mathcal{L}(M,V) \xrightarrow{\psi_*} \mathcal{L}(M,W)$$

Conversely suppose we have an exact chain of modules of the following form

$$U \xrightarrow{\varphi} V \xrightarrow{\psi} W \to 0$$

And recall the definition of the pull-back $\varphi^* : \mathcal{L}(V,M) \to \mathcal{L}(U,M)$ defined by $\varphi^*(g) = g\varphi$, then the following chain of R-modules is exact, as well

$$0 \to \mathcal{L}(W,M) \xrightarrow{\psi^*} \mathcal{L}(V,M) \xrightarrow{\varphi^*} \mathcal{L}(U,M)$$

The following theorem is somewhat of an inverse of the lemma above: It grants the exactness of the original chain of modules, iff all chains of homomorphism modules are exact. The proof just chooses clever candidates for modules L and N in order to establish the exactness of the original chain. However we will vastly generalize this statement in category theory in section 11.2.

(3.94) Lemma: (viz. 993)
Yoneda's Lemma: Let $(R,+,\cdot)$ be any ring, $n \geq 2$ and for any $i \in 1 \dots n$ consider a homomorphisms $\varphi_i : M_{i-1} \to M_i$ of R-modules. We will abbreviate the following chain of R-modules by $\star$

$$\star \;:=\; M_0 \xrightarrow{\varphi_1} M_1 \xrightarrow{\varphi_2} M_2 \to \dots \xrightarrow{\varphi_n} M_n$$

(i) If for any R-module L the following chain of R-modules is exact, then the original chain $\star$ already was exact, itself

$$\mathcal{L}(L,M_0) \xrightarrow{(\varphi_1)_*} \mathcal{L}(L,M_1) \xrightarrow{(\varphi_2)_*} \mathcal{L}(L,M_2) \to \dots \xrightarrow{(\varphi_n)_*} \mathcal{L}(L,M_n)$$

(ii) If for any R-module N the following chain of R-modules is exact, then the original chain $\star$ already was exact, itself

$$\mathcal{L}(M_n,N) \xrightarrow{(\varphi_1)^*} \mathcal{L}(M_{n-1},N) \to \dots \xrightarrow{(\varphi_2)^*} \mathcal{L}(M_1,N) \xrightarrow{(\varphi_1)^*} \mathcal{L}(M_0,N)$$

3.10 Rank of Modules

Remember that in section 3.7 we defined the **rank** of an R-module to be the minimal cardinality of a generating set of M. Formally that is the definition

$$\mathrm{rank}(M) \;:=\; \min\{\,|X| \mid X \subseteq M,\ M = \mathrm{Lh}(X)\,\}$$

That is: If $I = \mathrm{rank}(M)$ then there is some subset $\{\,m_i \mid i \in I\,\} \subseteq M$ that generates M as its linear hull $M = \mathrm{Lh}\{\,m_i \mid i \in I\,\}$. And conversely, if $X \subseteq M$ generates $M = \mathrm{Lh}(X)$, then $|I| \leq |X|$.
Be careful however - a *minimal set of generators*, need not have *minimal cardinality*! E.g. the set $\{\,2,3\,\} \subseteq \mathbb{Z}$ is a minimal set of generators of the $\mathbb{Z}$-module $\mathbb{Z}$. That is $\{\,2,3\,\}$ generates $\mathbb{Z} = \langle 2,3\rangle_{\mathsf{m}}$ and of course neither $\{2\}$ nor $\{3\}$ generates $\mathbb{Z}$. However we have $\mathrm{rank}(\mathbb{Z}) = 1$, as $\mathbb{Z} = \langle 1\rangle_{\mathsf{m}}$ is clear. As we have seen in (3.64.(iv)) this is quite different in the case of modules over skew-fields. But even the base ring $\mathbb{Z}$ (and what better ring is there to wish for?) gives rise to such peculiarities.
Let us now study the basic properties of the rank of modules, but be ready for some nasty surprises, as the theory will take some twists and turns. Many properties one would think of as evident will be untrue, unless we deal with nice rings and modules. Others will hold true in astounding generality.

(3.95) Example: (viz. 995)

(i) The ring $\mathbb{Z}$ is an UFD (in fact even a PID) that contains infinitely many prime elements. That is the following set contains infinitely elements

$$\mathbb{P} \;:=\; \{\,p \in \mathbb{Z} \mid 2 \leq p \text{ is prime}\,\}$$

(ii) The set $\mathbb{Q}$ regarded as an $\mathbb{Z}$-module is has no finite set of generators. Hence it is of countably infinite rank. A generating set is being given by

$$P \;:=\; \left\{\, \frac{1}{p^k} \mid p \in \mathbb{P}, k \in \mathbb{N} \,\right\}$$

(3.96) Proposition: (viz. 1001)
Let $(R,+,\cdot)$ be an arbitrary ring and consider any two R-modules M and N. If now $\varphi : M \twoheadrightarrow N$ is a surjective R-linear map (an R-module epimorphism), then N cannot exceed M in rank:

$$\mathrm{rank}(N) \;\leq\; \mathrm{rank}(M)$$

Likewise, if $P \leq_{\mathsf{m}} M$ is an R-sub-module of M, then we get the following inequality for the rank of M

$$\mathrm{rank}(M) \;\leq\; \mathrm{rank}(P) + \mathrm{rank}\left(M \Big/ P\right)$$

(3.97) Proposition: (viz. 1005)
Let $(R,+,\cdot)$ be a commutative, non-zero ring $R \neq 0$. If now M and N are free R-modules, then M and N are isomorphic as R-modules, if and only if they share the same rank, formally that is

$$M \;\cong_{\mathfrak{m}}\; N \quad\Longleftrightarrow\quad \operatorname{rank}(M) \;=\; \operatorname{rank}(N)$$

In particular: If M is free of rank $I = \operatorname{rank}(M)$, then M is isomorphic to the Euclidean R-module $M \cong_{\mathfrak{m}} R^{\oplus I}$ presented in (3.60). If $\{ m_i \mid i \in I \}$ is an R-basis of M, then an isomorphism is given by

$$R^{\oplus I} \;\xrightarrow{\sim}\; M \;:\; (a_i) \mapsto \sum_{i\in I} a_i m_i$$

(3.98) Remark:
The above proposition (3.96) enables us to control the rank of M by controling the rank of a sub-module $P \leq_{\mathfrak{m}} M$ (and of the quotient M/P). On the other hand one is tempted to expect that the rank of a sub-module P of M cannot exceed the rank of the containing module M. However nothing is farther from the truth. Consider the ring $R = \mathbb{Q}[t_i \mid i \in I]$ where I is an arbitrary index set. If $I = 1 \ldots n$ then we have the usual polynomial ring $\mathbb{Q}[t_1, \ldots, t_n]$ that is a very tame ring - a noetherian integral domain. If we now regard the ring $M = R$ as an R-module itself, it is clear, that $\operatorname{rank}(M) = 1$. However, hell breaks loose, once we take a look at the ideal $\mathfrak{m} := \langle t_i \mid i \in I \rangle_{\mathfrak{i}} \trianglelefteq_{\mathfrak{i}} R$. If we take $\mathfrak{m}$ as an R-sub-module of $M = R$, then the rank of $\mathfrak{m}$ is no less than

$$\operatorname{rank}(M) \;=\; 1 \;\leq\; |I| \;=\; \operatorname{rank}(\mathfrak{m})$$

By primary decomposition it is easy to see, that $T := \{ t_i \mid i \in I \}$ is a minimal generating set $\mathfrak{m} = \operatorname{Lh}_R(T)$ and in fact it hits the rank. That is the sub-module $\mathfrak{m}$ of M can have arbitrarily large rank, even though M is of rank 1! Modules can have astoundligly vast space within themselves! The reason is that all those t_i do not take up much space, they are all linearly dependent: $t_j t_i - t_i t_j = 0$.

So the question arises how to control the space *inside* a module. One of the best answers one can give refers to *free* sub-modules of M - these cannot be larger than M itself - refer to (3.99.(iv)). Also note that as long as I is finite R is noetherian. And in fact sub-modules of finitely generated modules over noetherian rings are again finitely generated. This will be the topic of section 3.11. Finally note that in case of $|I| = 1$ we even had $\operatorname{rank}(\mathfrak{m}) = \operatorname{rank}(M)$. But in this case R even is a PID and in fact finitely generated modules over PIDs are very well-behaved.

(3.99) Lemma: (viz. 1001)
Consider a commutative ring $(R,+,\cdot)$ and an R-module M. Further suppose, that $R \neq 0$ is non-zero. Then the following statements are true

(i) If $\{ x_1, \ldots, x_n \} \subseteq M$ (where $n \in \mathbb{N}$) generates M as an R-module, then any $n+1$ elements of M are R-linearly dependent. That is: Given $y_1, \ldots, y_n, y_{n+1} \in M$ there are some $a_1, \ldots, a_n, a_{n+1} \in R$ such that $a_k \neq 0$ for some $k \in 1 \ldots n+1$ and:

$$a_1 y_1 + \cdots + a_n y_n + a_{n+1} y_{n+1} \;=\; 0$$

(ii) If $\{ m_1, \ldots, m_n \} \subseteq M$ (where $n \in \mathbb{N}$) is an R-basis of M and $\{ x_1, \ldots, x_n \}$ generates M as an R-module, then $\{ x_1, \ldots, x_n \}$ is a basis, as well.

(iii) If $B \subseteq M$ is an R-basis of M then the cardinality of B equals the rank of M, formally that is

$$\text{rank}(M) \quad = \quad |B|$$

(iv) If $F \leq_{\mathsf{m}} M$ is a free sub-module of M, then it's rank does not exceed the rank of M, formally

$$\text{rank}(F) \quad \leq \quad \text{rank}(M)$$

(3.100) Remark:
Dimension: In general, for an arbitrary ring $(R, +, \cdot)$ and a free R-module M the **dimension** is set to be the minimal cardinality of an R-basis of M

$$\dim(M) \quad := \quad \min\{ \, |B| \mid B \subseteq M \text{ is a basis of } M \, \}$$

From this definition it is clear that the rank of M does not exceed the dimension of M [because any base B of M already generates $M = \text{Lh}(B)$], that is

$$\text{rank}(M) \quad \leq \quad \dim(M)$$

In this light lemma (3.99.(iii)) tells us that in case of a commutative ring R *all* bases of a free R-module M share the same cardinality, namely the rank of M. In particular - if R is commutative and M is free - we even have the equality of

$$\dim(M) \quad = \quad \text{rank}(M)$$

Thus - for commutative rings - the dimension is not a new invariant. However it is customary to refer to the dimension, rather than the rank, when operating with free modules. Also we have seen in (3.64.(vi)) that for any skew-field $(S, +, \cdot)$ and any S-vector-space V all bases share the same cardinality, as well. It is easy to see that this is the rank again

$$\dim(V) \quad = \quad \text{rank}(V)$$

Prob as $\text{rank}(V) \leq \dim(V)$ is always true, it remains to prove $\dim(V) \leq \text{rank}(V)$. Thus let $X \subseteq M$ be a generating set of M with $|X| = \text{rank}(M)$. Then by the basis selection theorem (3.58) there is a subset $B \subseteq X$ such that B is a basis of M. In particular $\dim(S) = |B| \leq |X| = \text{rank}(X)$.

After these two important cases, commutative rings and skew-fields, on might be tempted to think that generally (over arbitrary rings) all bases share the same cardinality, preferably the rank of M. This is untrue however. There are some modules over non-commutative rings, that have bases of different size. We have given one such example in (3.84).

(3.101) Definition:
Let $(R,+,\cdot)$ be an arbitrary ring and M be an R-module. Then a subset $L \subseteq M$ is said to be a **maximal linear independent set** of M, iff it is R-linearly independent and for any other R-linearly independent set $L' \subseteq M$ we get the implication

$$L \subseteq L' \implies L = L'$$

As we will see in (3.102.(viii)), if R is an integral domain then all maximal linear independent subsets of M are of the same cardinality. Hence in this case we may define the **linear freedom** of M to be

$$\text{free}(M) := |L| \text{ for some maximal linear independent set } L \subseteq M$$

(3.102) Corollary: (viz. 1005)
Let $(R,+,\cdot)$ be an arbitrary ring and M be an R-module. Then we obtain the following statements concerning maximal linear independent subsets of M

(i) Any linear independent set in M is contained in a maximal linear independent set. That is: If $L \subseteq M$ is R-linearly independent, then there is a maximal linear independent set $L^* \subseteq M$ with

$$L \subseteq L^*$$

(ii) If $R \neq 0$ is not the zero ring, L is a maximal linear independent set and $x \in M$ is any element of M, then there is some $a \in R$ satisfying the following property

$$a \neq 0 \quad \text{and} \quad ax \in \text{Lh}(L)$$

(iii) Recall that M is said to be a *torsion module*, iff for any $x \in M$ there is some $a \in R$, $a \neq 0$ such that $ax = 0$. If now R is an integral domain, then this property translates into

$$\text{free}(M) = 0 \iff M \text{ is a torsion module}$$

(iv) If $L \subseteq M$ is a linear independent set, then the sub-module $F := \text{Lh}(L)$ generated by L is a free R-module with basis L. In particular if $R \neq 0$ is a non-zero commutative ring then the cardinality of any any linear independent set L in M is bounded by the rank of M. That is

$$|L| \leq \text{rank}(M)$$

(v) Let R be an integral domain and $L \subseteq M$ be a linearly independent set in M. We denote by by $F := \text{Lh}(L) \leq_{\mathfrak{m}} M$ the free sub-module of M generated by L. Finally consider finitely many elements $x_1, x_2, \ldots, x_n \in M$ (where $n \in \mathbb{N}$) such that

- $M = F + \text{Lh}\{ x_1, x_2, \ldots, x_n \}$
- $\forall\, i \in 1 \ldots n : L \cup \{x_i\}$ is linearly dependent

Then L is a maximal linearly independent subset of M, M/F is a torsion module and in particular the linear freedom of M equals the dimension of F:

$$\mathrm{free}(M) \;=\; |L| \;=\; \dim(F)$$

(vi) In a more fancy language (ii) can be put as: If $R \neq 0$ is a non-zero ring and L is a maximal linear independent set, with $F := \mathrm{Lh}(L)$ then the quotient M/F is a torsion R-module. That is

$$\forall\, z \in M\big/_F \;\; \exists\, a \in R \;\text{ such that } a \neq 0 \;\text{ and } az = 0$$

Conversely if $F \leq_{\mathsf{m}} M$ is a free sub-module of M such that the quotient M/F is a torsion module, then any basis $B \subseteq F$ is a maximal linear independent set $B \subseteq M$ in M.

(vii) Let now R even be an integral domain and consider a linearly independent set $L \subseteq M$. Further for any $x \in L$ let $a_x \in R$ be any non-zero element $a_x \neq 0$ of R. Then the set $L' := \{\, a_x x \mid x \in L \,\}$ is linearly independent again and $|L| = |L'|$.

(viii) If R even is an integral domain, then any two maximal linear independent sets have the same cardinality. That is: If K and $L \subseteq M$ are any two maximal linear independent sets, then

$$|K| \;=\; |L| \;\leq\; \mathrm{rank}(M)$$

(ix) If R is an integral domain and $P \leq_{\mathsf{m}} M$ is any sub-module of M, then linear freedom of M equals the sum of the linear freedoms of P and the quotient M/P, formally that is

$$\mathrm{free}(M) \;=\; \mathrm{free}(P) + \mathrm{free}\left(M\big/_P\right)$$

(x) $(\diamondsuit)$ Let R be an integral domain and denote its quotient field by $E := \mathrm{QUOT}(R)$. Then the linear freedom of M is just the dimension of the scalar extension of M to E, formally that is

$$\mathrm{free}_R(M) \;=\; \dim_E(E \otimes_R M)$$

(3.103) Remark:

(i) It is clear that in the case of a free R-module M over an integral domain R the linear freedom equals the dimension, as any basis of M already is a maximal linear independent subset

$$M \text{ free} \;\Longrightarrow\; \mathrm{free}(M) \;=\; \dim(M)$$

However, if M is not free, then the rank of M may well be larger, than the linear freedom. The following two examples (ii) and (iii) should enlighten the situation

$$\text{gererally} \;\Longrightarrow\; \mathrm{free}(M) \;\leq\; \mathrm{rank}(M)$$

(ii) Consider the $\mathbb{Z}$-module $M := \mathbb{Z}^f \oplus (\mathbb{Z}_n)^k$ for some arbitrary numbers $f, k \in \mathbb{N}$. As $F := \mathbb{Z}^f \oplus 0$ is a free sub-module $F \leq_{\mathfrak{m}} M$ and $M/F = 0 \oplus (\mathbb{Z}_n)^k$ is a torsion module (3.102.(vi)) implies that the linear freedom of M is precisely f. However $(\mathbb{Z}_n)^k$ contributes to the rank of M and hence

$$f \;=\; \text{free}(M) \;\leq\; \text{rank}(M) \;=\; f + k$$

This is to be interpreted in the following way: The rank yields a more accurate description of the module, hence (3.97) - it regards every part of M. The linear freedom only is the dimension of the largest free module inside M, it neglects components with torsion. This makes it is easier to control, whereas the rank can explode incontrollably by picking up torsion. Just compare (3.102.(ix)) to (3.96), the inequality now is an equality.

(iii) Consider the integral domain $R := \mathbb{Z}[t]$ and regard the (maximal) ideal $\mathfrak{m} := \langle 2, t \rangle_{\mathfrak{i}} \trianglelefteq_{\mathfrak{i}} R$ as an R-module. Then $\mathfrak{m}$ has a linear freedom of 1, as $\{t\}$ is a maximal linear independent set (any other $f \in R$ would yield a linearly dependent set). The rank is 2 however ($\mathfrak{m}$ is not a principal ideal). This can happen, as $R/\mathfrak{m} \cong_{\mathfrak{m}} \mathbb{Z}_2$ has torsion. Also note that $\mathfrak{m}$ is not a free module, just because it is not a principal ideal.

(3.104) Theorem: (viz. 1009)
Modules over PIDs: Let $(R, +, \cdot)$ be a PID and let M be a module over R. If now $P \leq_{\mathfrak{m}} M$ is any sub-module of M, then we get the following statements

(i) If M is free, then P is free, as well and its dimension does not exceed the dimension of M, that is

$$\dim(P) \;\leq\; \dim(M)$$

(ii) If M is finitely generated, then P is finitely generated, as well. Generally the rank of P does not exceed the rank of M. That is

$$\text{rank}(P) \;\leq\; \text{rank}(M)$$

(iii) If M is finitely generated, then M is free if and only if it is torsion free. That is we have the equivalence of the statements

$$M \text{ free} \quad\Longleftrightarrow\quad \text{TOR}(M) \;=\; 0$$

(iv) If M is finitely generated, then M is isomorphic to the (exterior) direct sum of the free R-module $M/\text{TOR}(M)$ and the torsion-module $\text{TOR}(M)$. Formally again

$$M \;\cong_{\mathfrak{m}}\; M \Big/ _{\text{TOR}(M)} \oplus \text{TOR}(M)$$

(3.105) Remark:

(i) In section (3.7) we have seen that, if R is a skew-field, then any R-module M is free already. In particular any sub-module $P \leq_{\mathfrak{m}} M$ is free, as well. Thus, concerning skew-fields, we have not gained something new, but R has been a PID here.

(ii) If R is not a PID, then this result need not be true! Consider the base ring $R = \mathbb{Z}[s,t]$. Note that this ring is a noetherian integral domain, the next-best thing apart from a PID. We take $M = R$ to be the free R-module of rank 1. Then the sub-module $P := \mathrm{Lh}\{ s,t \}$ is not free, as it contains the linear dependence $t \cdot s - s \cdot t = 0$. And P also has rank 2 over R.

(iii) The proof of this theorem uses the well-known but rarely used *well-ordering theorem* (0.30), that is a consequence of the axiom of choice (in fact it even is equivalent to the AC on the basis of the other axioms of set-theory). It states, that on any non-empty set I there is a total order $\leq$ that such that every non-empty subset $H \subseteq I$ contains a minimal element. Formally for any $H \subseteq I$ with $H \neq \emptyset$ there is some $m \in H$ such that for any $h \in H$ we get $h \leq m \implies h = m$. In case of a finite set $I = \{ i_1, \ldots, i_n \}$ this is evident, just define $\leq$ to be any linear order $i_1 < i_2 < \cdots < i_n$ of these elements. But in fact such an order exists for arbitrarily large sets I, which might come as a little surprise.

(iv) In fact the proof shows a little more: If $\{ m_i \mid i \in I \}$ is a basis of M, then there is a subset $H \subseteq I$ of I such that we find a basis $\{ p_i \mid i \in H \}$ of P, where any p_j ($j \in H$) is of the form

$$p_j \;=\; a_j m_j + \sum_{i<j} b_{i,j} m_i$$

for some coefficients a_j and $b_{i,j} \in R$. We will be able to refine this result for finitely generated R-modules, by precisely describing their structure (up to isomorphy).

3.11 Noetherian Modules

In the previous section we have seen, that the size (in terms of the *rank*) of a sub-module P of M can be very hard to control. However there are those well-behaved modules for which the rank remains finite at last. If $M = R$ is the base ring itself, the sub-modules of M are the ideals of M. And a ring in which all ideals are finitely generated has been called *noetherian*. So we will generalize this notion to the case of modules over a commutative ring and it turns out *noetherian* modules have a whole bunch of nice properties that we are about to explore:

(3.106) Definition: (viz. 891)
Let $(R, +, \cdot)$ be a commutative ring and M be an R-module. Then M is said to be a **noetherian** module, iff it satisfies one of the following three equivalent conditions:

(a) M satisfies the *ascending chain condition* of sub-modules - that is every ascending chain of sub-modules of M becomes stationary. I.e. any sequence (P_k) (where $k \in \mathbb{N}$) of sub-modules $P_k \leq_{\mathsf{m}} M$ that satisfies

$$P_0 \subseteq P_1 \subseteq \ldots \subseteq P_k \subseteq P_{k+1} \subseteq \ldots$$

becomes eventually constant - that is there is some $s \in \mathbb{N}$, such that the chain actually looks like

$$P_0 \subseteq P_1 \subseteq \ldots \subseteq P_s = P_{s+1} = \ldots$$

(b) Every non-empty family $\mathcal{P} \subseteq \mathrm{Subm}(M)$, $\mathcal{P} \neq \emptyset$ of sub-modules of M contains a maximal element. I.e. there is some $P^* \in \mathcal{P}$ that satisfies the property

$$\forall\, P \in \mathcal{P} \;:\; P^* \subseteq P \implies P = P^*$$

(c) Every sub-module P of M is finitely generated. That is for any sub-module $P \leq_{\mathsf{m}} M$ there are some $\{ x_1, \ldots, x_n \} \subseteq P$, that generate P as an R-module

$$P = \mathrm{Lh}(x_1, \ldots, x_n)$$

(3.107) Definition:
Let $(R, +, \cdot)$ be a commutative ring and M be an R-module. Then M is said to be a **artinian** module, iff it satisfies one of the following two equivalent conditions:

(a) M satisfies the *descending chain condition* of sub-modules - that is every descending chain of sub-modules of M becomes stationary. I.e. any sequence (P_k) (where $k \in \mathbb{N}$) of sub-modules $P_k \leq_{\mathsf{m}} M$ that satisfies

$$P_0 \supseteq P_1 \supseteq \ldots \supseteq P_k \supseteq P_{k+1} \supseteq \ldots$$

becomes eventually constant - that is there is some $s \in \mathbb{N}$, such that the chain actually looks like

$$P_0 \supseteq P_1 \supseteq \ldots \supseteq P_s = P_{s+1} = \ldots$$

(b) Every non-empty family $\mathcal{P} \subseteq \mathrm{Subm}(M)$, $\mathcal{P} \neq \emptyset$ of sub-modules of M contains a minimal element. I.e. there is some $P_* \in \mathcal{P}$ such that

$$\forall\, P \in \mathcal{P} \;:\; P \subseteq P_* \implies P = P_*$$

Prob the equivalence of these statements is no specialty of modules, but a general truism for partial orders. In this case the order in question is $P \leq Q$ defined by $Q \subseteq P$. Then this equivalence here is just an application of (0.25).

(3.108) Remark:
The notion of a noetherian (resp. artinian) module is closely related to the notion of a noetherian (resp. artinian) ring. In fact if we regard a commutative ring R as a module over itself, then the ideals $\mathfrak{a} \trianglelefteq_{\mathsf{i}} R$ are precisely the sub-modules $\mathfrak{a} \leq_{\mathsf{m}} R$ of R. Hence by property (a) we see, that R is noetherian (resp. artinian) as an R-module, if and only if it is noetherian (resp. artinian), as a ring.

(3.109) Example:
Clearly $\mathbb{Z}$ is a noetherian ring (it even is a PID) and hence a noetherian $\mathbb{Z}$-module. However $\mathbb{Z}$ is not artinian, as there is an infinitely descending chain of ideals, that does not stabilize, given by

$$\mathbb{Z} \supset 2\mathbb{Z} \supset 4\mathbb{Z} \supset \ldots \supset 2^k\mathbb{Z} \supset \ldots$$

Conversely pick up any prime $p \in \mathbb{Z}$ and regard the sub-ring $\mathbb{Z}[1/p] \leq_{\mathsf{r}} \mathbb{Q}$ of $\mathbb{Q}$ generated by $1/p \in \mathbb{Q}$. Clearly $\mathbb{Z} \leq_{\mathsf{r}} \mathbb{Z}[1/p]$ is a sub-ring as well, and hence a sub-module. Therefore we may regard the quotient module of $\mathbb{Z}[1/p]$ by $\mathbb{Z}$ as a $\mathbb{Z}$-module again

$$I(p) \;:=\; \mathbb{Z}[1/p] \,\big/\, \mathbb{Z} \;=\; \left\{ x + \mathbb{Z} \mid \exists\, k \in \mathbb{N} : p^k x \in \mathbb{Z} \right\}$$

By the way, this is just the p-primary component of $\mathbb{Q}/\mathbb{Z}$. Then $I(p)$ is not noetherian, as there is an infinitely ascending chain of sub-modules of $I(p)$, that does not stabilize

$$\mathbb{Z} \subset \mathbb{Z}\left(\frac{1}{p} + \mathbb{Z}\right) \subset \mathbb{Z}\left(\frac{1}{p^2} + \mathbb{Z}\right) \subset \mathbb{Z}\left(\frac{1}{p^3} + \mathbb{Z}\right) \subset \ldots$$

However it can be shown, that $I(p)$ is a artinian module. Recall that in the case of commutative rings, any artinian ring already is noetherian. Yet $I(p)$ is *not* noetherian: In the case of modules, artinian does not imply noetherian and artinian modules need not be finitely generated!

(3.110) Example: (viz. 894)

- Let us consider the rationals $\mathbb{Q}$ as a $\mathbb{Z}$-module canonically. Then for any $0 \neq b \in \mathbb{Z}$ we clearly get a sub-module of $\mathbb{Q}$ by virtue of

$$M_b \;:=\; \mathbb{Z}\frac{1}{b} \;=\; \left\{ \frac{a}{b} \;\middle|\; a \in \mathbb{Z} \right\}$$

And any finitely generated sub-module P of $\mathbb{Q}$ is contained in a sub-module of this kind. But M_b is not $\mathbb{Q}$, e.g. it lacks $1/2b$, so that we can conclude, that $\mathbb{Q}$ is not finitely generated, as a $\mathbb{Z}$-module.

- If $a \mid b$, say $au = b$ than $1/a = u/b \in M_b$ such that $M_a \subseteq M_b$. If now p is any prime number, then we therefore find an infinitely ascending chain of sub-modules of $\mathbb{Q}$ (i.e. $\mathbb{Q}$ is not *noetherian*)

$$\mathbb{Z} \;=\; M_1 \;\subset\; M_p \;\subset\; M_{p^2} \;\subset\; M_{p^3} \;\subset\; \ldots$$

- Another kind of $\mathbb{Z}$-sub-module of $\mathbb{Q}$ is given by the following construction: Choose a prime number p, then the set D_p of all fractions whose denominator is *not* divisible by p is a sub-module of $\mathbb{Q}$:

$$D_p \;:=\; \left\{ \frac{a}{b} \in \mathbb{Q} \;\middle|\; p \not| \, b \right\}$$

 In fact this is just the localization $\mathbb{Z}_{(p)} := \mathbb{Z}_{\mathfrak{p}}$ where $\mathfrak{p} = p\mathbb{Z}$, but $D_p \;\leq_{\mathsf{m}}\; \mathbb{Q}$ can also be seen elementary: If a/b and $c/d \in D_p$, then $a/b + c/d = (ad + bc)/(ad)$. Suppose $p \mid ad$, then, since p is prime we had $p \mid a$ or $p \mid d$, which are both untrue, by assumption, hence $a/b + c/d \in D_p$ again. And $k(a/b) = (ka)/b \in D_p$ is clear, for any $k \in \mathbb{Z}$ and $a/b \in D_p$. Thus D_p is closed under addition and scalar multiplication, i.e. a submudule.

- The same construction holds true for any set $P \subseteq \mathbb{Z}$ of prime numbers, let D_P be the set of all fractions whose denominator is *not* divisible by any prime $p \in P$

$$D_P \;:=\; \left\{ \frac{a}{b} \in \mathbb{Q} \;\middle|\; \forall\, p \in P : p \not| \, b \right\} \;=\; \bigcap_{p \in P} D_p$$

 Then by the same reasoning as above it is clear that D_P is a sub-module of $\mathbb{Q}$. And trivially we have $D_Q \subseteq D_P$ whenever $P \subseteq Q \subseteq \mathbb{Z}$ are sets of prime numbers. Thus we also find an infinitely descending chain of sub-modules in $\mathbb{Q}$ (i.e. $\mathbb{Q}$ is not *artinian*)

$$\ldots \;\subset\; D_{\{2,3,5\}} \;\subset\; D_{\{2,3\}} \;\subset\; D_2 \;\subset\; D_\emptyset \;=\; \mathbb{Q}$$

- In the proof we present a reasoning that shows, that $\mathbb{Q}$ does not contain any proper, maximal $\mathbb{Z}$-sub-module. That is: If $U \;\leq_{\mathsf{m}}\; \mathbb{Q}$ is a sub-module with $P \neq \mathbb{Q}$, then there always is another sub-module $V \;\leq_{\mathsf{m}}\; \mathbb{Q}$ in between: $U \subset V \subset \mathbb{Q}$. In this sense the space inside $\mathbb{Q}$, if we regard it as a $\mathbb{Z}$-module, is infinte.

(3.111) Theorem: (viz. 892)
Let $(R, +, \cdot)$ be a commutative ring and M, N be R-modules. We also regard two sub-modules P, $Q \;\leq_{\mathsf{m}}\; M$ of M. In order to avoid giving two completely analogous lists of theorems, let us abbreviate

$$\star \;\in\; \{\, \text{noetherian, artinian} \,\}$$

(i) M is a $\star$ module if and only if both P and the quotient M/P are $\star$ modules. Formally that is

$$M \text{ is } \star \quad\Longleftrightarrow\quad P \text{ and } {}^{M}\!\Big/_{P} \text{ are } \star$$

(ii) If both quotient modules M/P and M/Q are $\star$ modules, then the quotient $M/(P \cap Q)$ is a $\star$ module again. Formally that is the implication

$$M\Big/_P \text{ and } M\Big/_Q \text{ are } \star \implies M\Big/_{P\cap Q} \text{ is } \star$$

(iii) If both P and Q are $\star$ modules, then so is their sum $P+Q \leq_{\mathfrak{m}} M$. Formally that is the implication

$$P \text{ and } Q \text{ are } \star \implies P+Q \text{ is } \star$$

(iv) If both M and N are $\star$ modules, then the direct sum $M \oplus N$ of M and M is a $\star$ module again and vice versa. Formally that is the equivalence

$$M \text{ and } N \text{ are } \star \iff M \oplus N \text{ is } \star$$

(v) The epimorphic image of a $\star$ module is $\star$ again. That is: If $\varphi : M \to N$ is a surjective homomorphism of R-modules and M is a $\star$ module, then so is N. Formally that is the implication

$$M \twoheadrightarrow N \text{ and } M \text{ is } \star \implies N \text{ is } \star$$

(vi) If M is a finitely generated R-module and R is a $\star$ ring, then M already is a $\star$ module. Formally

$$M \text{ finitely generated and } R \text{ is } \star \implies M \text{ is } \star$$

(vii) If L, M and N are R-modules and $0 \to L \to M \to N \to 0$ is a short exact sequence of R-modules, then we get the equivalence of the statements

$$M \text{ is } \star \iff L \text{ and } N \text{ are } \star$$

(3.112) Remark:
It is clear that the above statements (ii), (iii) and (iv) can be generalized to finitely many (sub)-modules. E.g. if P_1 to $P_n \leq_{\mathfrak{m}} M$ are finitely many sub-modules of M, then we obtain the following implication

$$\forall\, i \in 1 \ldots n \,:\, M\Big/_{P_i} \text{ is } \star \implies M\Big/_{P_1 \cap P_2 \cap \cdots \cap P_n} \text{ is } \star$$

Prob this can be easily seen by induction on n: The case $n = 1$ is trivial and for the induction step just let $P := P_1$ and $Q := P_2 \cap \cdots \cap P_n$ and use the respective theorem.
The following proposition shows that in case of vector spaces there is no difference between artinian and noetherian modules, as both are the finiteness of the dimension of the vector space. We will generalize this theorem soon, but in order to do this we first have to find a suitable substitute for the dimension, in case the module in question is not over a field. This notion will be the *length*, an invariant that controls the maximal number of subspaces that can be stacked in M. So let us start with this easy to prove

(3.113) Proposition: (viz. 894)
Let $(F, +, \cdot)$ be a field and V be an F-vector space. Then V is noetherian resp. artinian if and only if it is finite dimensional. That is the following three statements are equivalent:

(a) V is artinian

(b) V is noetherian

(c) V is finite-dimensional

(3.114) Definition: (viz. 895)
Let $(R, +, \cdot)$ be an arbitrary ring and M be an R-module. Then M is said to be a **simple** R-module if $M = 0$ and M has no proper sub-modules. That is $M = 0$ and it satisfies one of the following two equivalent properties:

(a) For any sub-module $P \leq_{\mathfrak{m}} M$ of M we either have $P = 0$ or $P = M$

(b) Any non-zero element of M generates M as an R-module, that is for any $x \in M$ with $x \neq 0$ we already get $M = Rx$.

And if R is commutative, we obtain the following third equivalent statement

(c) There is some maximal ideal $\mathfrak{m} \trianglelefteq_{\mathfrak{i}} R$ of R such that M is isomorphic to the quotient ring $R/\mathfrak{m}$ as an R-module, formally that is

$$\exists\, \mathfrak{m} \in \operatorname{Smax}(R) \text{ such that } M \cong_{\mathfrak{m}} R \Big/ \mathfrak{m}$$

Let $(R, +, \cdot)$ be an arbitrary ring and M be an R-module. Then M is said to be **semi-simple**, iff M can be decomposed into a direct sum of simple sub-modules. That is there is an arbitrary family $M_i \leq_{\mathfrak{m}} M$ of sub-modules (where $i \in I$), such that M_i is a simple R-module (for any $i \in I$) and M is the inner direct sum of these simple sub-modules M_i

$$M = \bigoplus_{i \in I} M_i$$

(3.115) Definition:
Let $(R, +, \cdot)$ be a commutative ring and M be an R-module. Then the tuple $(M_0, M_1, \ldots, M_r)$ is said to be a **composition series** of M, iff the M_i form an ascending chain of sub-modules $M_i \leq_{\mathfrak{m}} M$

$$0 = M_0 \subset M_1 \subset \ldots \subset M_r = M$$

such that for any $i \in 1 \ldots r$ the quotient module M_i / M_{i-1} is simple. And by (3.114) this can be put as: For any $i \in 1 \ldots r$ and any sub-module $P \leq_{\mathfrak{m}} M$ of M we get the following implication

$$M_{i-1} \subseteq P \subseteq M_i \implies P = M_{i-1} \text{ or } P = M_i$$

If M admits a composition series $(M_0, M_1, \ldots, M_r)$ then M is said to be of *finite length*. And we will see in (3.117.(iii)) that in this case the length r of the series is uniquely determined. Hence this number will be called the **length** of the module M, denoted by

$$\ell(M) \;:=\; r \;\in\; \mathbb{N}$$

And in case M admits no (or no finite) composition series we say that M is of *infinite length* and we denote this situation, by writing

$$\ell(M) \;:=\; \infty$$

(3.116) Remark:

(i) If $\ell(M) = 0$ then $0 = M_0 = M$, that is M is the zero-module. And clearly if $M = 0$ is zero, then (0) is the only available composition series. Hence there is the equivalence

$$\ell(M) \;=\; 0 \quad\Longleftrightarrow\quad M \;=\; 0$$

(ii) If $\ell(M) = 0$ then $0 = M_0 \subset M_1 = M$ is a composition series, that is $M = M/0 = M_1/M_0$ is a simple R-module. Conversely if M is simple then $(0, M)$ already is the one and only composition series of M, such that

$$\ell(M) \;=\; 1 \quad\Longleftrightarrow\quad M \text{ is simple}$$

(iii) We will often use the following trick: If N is a simple R-module and $\iota : M \hookrightarrow N$ is an R-module monomorphism, then already $M = 0$ or $\iota : M \xrightarrow{\sim} N$ even is an isomorphism.

Prob let $Q := \mathrm{im}(\iota) \leq_{\mathsf{m}} N$ be the image of M in N. Then, as N is simple, we either have $Q = 0$ or $Q = N$. But as ι is injective $\mathrm{im}(\iota) = 0$ implies $M = \iota^{-1}(0) = 0$ and $\mathrm{im}(\iota) = N$ means that ι is surjective and hence an isomorphism $\iota : M \xrightarrow{\sim} N$.

(iv) Another trick is the following observation: If M is a simple R-module and $\varrho : M \twoheadrightarrow N$ is an R-module-epimorphism, then already $N = 0$ or $\varrho : M \xrightarrow{\sim} N$ even is an isomorphism.

Prob let $P := \mathrm{kn}(\varrho) \leq_{\mathsf{m}} M$ be the kernel of ϱ in M. Then, as M is simple, we either have $P = 0$ or $P = M$. But $\mathrm{kn}(\varrho) = 0$ implies that ϱ is injective (and hence an isomorphism $\varrho : M \xrightarrow{\sim} N$) and $\mathrm{kn}(\varrho) = M$ implies $N = \mathrm{im}(\varrho) = 0$.

(v) If V is a finite-dimensional vectorspace over some field E then the length of V is not a new invariant, it simply equals the the dimension of V, that is

$$\ell(V) \;=\; \dim(V)$$

Prob let $\{ v_1, \ldots, v_n \} \subseteq V$ be a basis of V, then we denote the subspaces $V_i := \mathrm{Lh}(v_1, \ldots, v_i)$ of V for $i \in 0 \ldots n$. Then we find $E \cong_{\mathsf{v}} V_i/V_{i-1} : a \mapsto av_i + V_{i-1}$ such that V_i/V_{i-1} is simple. Hence $(V_0, V_1, \ldots, V_n)$ is a composition series of V and in particular $\ell(V) = n$.

(vii) If V is a vector-space over the skew-field $(S,+,\cdot)$ and $x \in V$ is any non-zero element $x \neq 0$ of V. Then clearly $Sx \subseteq V$ is a simple sub-module of V. In particular V already is semi-simple. To see this simply choose a basis $B \subseteq V$ of V, then V can be decomposed, into

$$V \;=\; \bigoplus_{b \in V} Sb$$

(3.117) Theorem: (viz. 895) **Jordan-Hölder Theorem**
Let $(R,+,\cdot)$ be a commutative ring and M be an R-module of finite length $\ell(M) < \infty$ (that is M admits a composition series). Then we obtain the following statements

(i) If $P \;\leq_{\mathfrak{m}}\; M$ is a sub-module of M with $P \neq M$, then the length of M exceeds the length of P, formally that is

$$\ell(P) \;<\; \ell(M)$$

(ii) If M is an arbitrary R-module and $P \leq M$ is any sub-module of M then M has finite length if and only if both P and the quotient M/P are of finite length, formally that is

$$M \text{ has finite length} \quad\Longleftrightarrow\quad P \text{ and } M\Big/P \text{ have finite length}$$

And in this case we even obtain the following equality for the length of the modules involved

$$\ell(M) \;=\; \ell(P) + \ell\left(M\Big/P\right)$$

More generally, if $0 = P_0 \subseteq P_1 \subseteq P_2 \subseteq \ldots \subseteq P_n = M$ is an ascending chain of sub-modules of M, then we find the equality

$$\ell(M) \;=\; \sum_{k=1}^{n} \ell\left(P_k\Big/P_{k-1}\right)$$

(iii) Any two composition series of M are *equivalent*: That is, given any two composition series $(M_0, M_1, \ldots, M_r)$ and $(N_0, N_1, \ldots, N_s)$ of M, then we get $r = s$ and there is a permutation $\sigma \in S_r$ such that for any $i \in 1 \ldots r$ there is an isomorphy

$$M_i\Big/M_{i-1} \;\cong_{\mathfrak{m}}\; N_{\sigma(i)}\Big/N_{\sigma(i)-1}$$

(iv) Let us denote the set of all strictly increasing chains of sub-modules of M, that start in 0 and terminate in M by $\mathcal{C}(0,M)$, that is

$$\mathcal{C}(0,M) \;:=\; \left\{ (P_0, P_1, \ldots, P_r) \;\middle|\; \begin{array}{l} \forall\, i \in 0 \ldots r : P_i \;\leq_{\mathfrak{m}}\; M \\ 0 = P_0 \;\subset\; P_1 \;\subset\; \ldots \;\subset\; P_r = M \end{array} \right\}$$

Then we obtain a partial order $\leq$ on $\mathcal{C}(0,M)$ by virtue of the following definition: Given two chains $(P_0, P_1, \ldots, P_r)$ and $(Q_0, Q_1, \ldots, Q_s)$ we say that $(P_0, P_1, \ldots, P_r) \leq (Q_0, Q_1, \ldots, Q_s)$ iff $r \leq s$ and there is an injective map $\alpha : 0 \ldots r \hookrightarrow 0 \ldots s$ with $\alpha(0) < \alpha(1) < \cdots < \alpha(r)$ such that for any $i \in 0 \ldots r$ we get

$$P_i \;=\; Q_{\alpha(i)}$$

And thereby, if $(M_0, M_1, \ldots, M_r) \in \mathcal{C}(0, M)$ is a strictly increasing chain of sub-modules of M the following statements are equivalent

(a) $r = \ell(M)$

(b) $(M_0, M_1, \ldots, M_r)$ is maximal

(c) $(M_0, M_1, \ldots, M_r)$ is a composition series

(v) Any strictly increasing chain of sub-modules of M can be *refined* into a composition series: That is, if $P_0 \subset P_1 \subset \ldots \subset P_k$ is a strictly increasing chain of sub-modules $P_i \leq_{\mathsf{m}} M$, then there is a composition series $(M_0, M_1, \ldots, M_r)$ of M such that (in the sense of (iv) above) we get

$$(P_0, P_1, \ldots, P_k) \quad \leq \quad (M_0, M_1, \ldots, M_r)$$

(vi) Consider a finite chain of R-modules M_i where $i \in 0 \ldots n$ and homomorphisms $\varphi_i : M_{i-1} \to M_i$ for $i \in 1 \ldots n$. That is for any $i \in 2 \ldots n$ we have $\varphi_i \varphi_{i-1} = 0$

$$0 \xrightarrow{\varphi_0} M_0 \xrightarrow{\varphi_1} M_1 \xrightarrow{\varphi_2} \ldots \xrightarrow{\varphi_n} M_n \xrightarrow{\varphi_{n+1}} 0$$

Then we obtain: If for any $i \in 0 \ldots n$ the module M_i is of finite length and H_i denotes the i-th homology module $H_i := \mathsf{kn}(\varphi_{i+1})/\mathsf{im}(\varphi_i)$ then we get the equality

$$\sum_{i=0}^{n} (-1)^i \ell(M_i) \quad = \quad \sum_{i=0}^{n} (-1)^i \ell(H_i)$$

(3.118) Remark:
The theorem of Jordan-Hölder part (ii) has some easy to get, yet very noteworthy consequences: Let L, M and N be modules over some commutative ring $(R, +, \cdot)$ again then

(i) If $\varphi : M \twoheadrightarrow N$ is a surjective homomorphism and M has finite length, then N also has finite length and we find the upper bound

$$\ell(N) \quad \leq \quad \ell(M)$$

Prob Let $P := \mathsf{kn}(\varphi)$, then $N \cong_{\mathsf{m}} M/P$ by the first isomorphism theorem and hence N is of finite length and satisfies $\ell(M) = \ell(P) + \ell(N)$ according to (3.117.(ii))

(ii) If $0 \to L \to M \to N \to 0$ is a (short) exact chain of R-modules and L and M are of finite length, then the length of M is the sum of the lengths of L and N

$$\ell(M) \quad = \quad \ell(L) + \ell(N)$$

Prob Say $\varphi : L \to M$ and $\psi : M \to N$, as the chain is exact we have $L' := \mathsf{im}(\varphi) = \mathsf{kn}(\psi) \leq_{\mathsf{m}} M$. And as φ is injective $L \cong_{\mathsf{m}} L'$ and as ψ is surjective also $N = \mathsf{im}(\psi)$. Combining all this, we get $M/L' = M/\mathsf{kn}(\psi) \cong_{\mathsf{m}} \mathsf{im}(\psi) = N$ and hence find, by (3.117.(ii)) again

$$\ell(M) \;=\; \ell(L') + \ell\left(M \Big/ L'\right) \;=\; \ell(L) + \ell(N)$$

(iii) If both M and N are of finite length, then the length of $M \oplus N$ is the sum of those of M and N:

$$\ell(M \oplus N) \;=\; \ell(M) + \ell(N)$$

Prob We obtain a short exact chains of R-modules $0 \to M \to M \oplus N \to N \to 0$ by using the homomorphsims $\iota : M \hookrightarrow M \oplus N : x \mapsto (x,0)$ and $\pi : M \oplus N \twoheadrightarrow N : (x,y) \mapsto y$. So the equality of length is just a special case of (ii) above.

(iv) If $0 = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_n = M$ is any increasing chain of sub-modules of M, then M has finite length, if and only if for any $k \in 1 \ldots n$ the quotient module M_k/M_{k-1} has finite length, and in this case the length of M is given to be

$$\ell(M) \;=\; \sum_{k=1}^{n} \ell\left(M_k \Big/ M_{k-1}\right)$$

Prob by induction on n: In case $n = 1$ we have $M = M/0 = M_1/M_0$. Now for the induction step: By (3.117.(ii)) M has finite length iff both M_{n-1} and $Q_n := M_n/M_{n-1}$ are of finite length and in this case we find $\ell(M) = \ell(M_{n-1}) + \ell(Q_n)$. If we now use the induction hypothesis on M_{n-1} we find the claim.

(3.119) Corollary: (viz. 901)
Let $(R,+,\cdot)$ be a commutative ring and M be an R-module, then we obtain the following statements

(i) M is noetherian, if and only if M is finitely generated and $R/\mathrm{ann}(M)$ is a noetherian ring, formally

$$M \text{ noetherian} \iff \mathrm{rank}(M) < \infty \text{ and } R \Big/ \mathrm{ann}(M) \text{ noetherian}$$

(ii) Under the assumption that M is finitely generated: M is artinian, if and only if $R/\mathrm{ann}(M)$ is an artinian ring, formally that is

$$M \text{ artinian} \iff R \Big/ \mathrm{ann}(M) \text{ artinian}$$

(iii) If M is a finitely generated, artinian R-module, then M already is an noetherian R-module, as well. Formally this is the implication

$$M \text{ artinian and finitely generated} \implies M \text{ noetherian}$$

(iv) If M is noetherian and $\varphi : M \to M$ is an R-module-endomorphism, then if φ is surjective, it already is bijective, that is the equivalence of

$$\varphi \text{ is surjective} \iff \varphi \text{ is bijective}$$

Nota in fact we have already proved this statement for any finitely generated module M over a general commutative ring R in (3.82). However the proof of the general case requires much more effort than the proof of this statement here.

(v) If M is artinian and $\varphi : M \to M$ is an R-module-endomorphism, then if φ is injective, it already is bijective, that is

$$\varphi \text{ is injective} \iff \varphi \text{ is bijective}$$

(vi) A module M is both artinian and noetherian, if and only if M is a module of finite length, formally

$$M \text{ artinian and noetherian} \iff \ell(M) < \infty$$

(vii) If R is an artinian ring, then the following 4 statements are equivalent

(a) M is artinian

(b) M is noetherian

(c) M is finitely generated

(d) M has finite length: $\ell(M) < \infty$

(viii) Let us now generalize proposition (3.113): If M is a semi-simple R-module (e.g. a vector space over a field), then the following 5 statements are equivalent:

(a) M is artinian

(b) M is noetherian

(c) M is finitely generated

(d) M has finite length: $\ell(M) < \infty$

(e) M is a finite direct sum of simple R-modules, that is there are finitely many ($i \in 1 \dots r$) simple sub-modules $M_i \leq_{\mathsf{m}} M$ of M such that $M = M_1 \oplus \cdots \oplus M_r$

M is finitely generated, iff $\operatorname{rank}(M) < \infty$, hence in case M even is a vector-space, that is R even is a field, we obtain the following sixth equivalent statement of (a) to (e) above:

(f) M is finite-dimensional: $\dim(M) < \infty$

(ix) Suppose M is a finitely generated R-module, such that every ascending chain of ideal-induced sub-modules of M stabilizes, then M is noetherian. That is: Suppose for every sequence of ideals $(\mathfrak{a}_k)$ where $\mathfrak{a}_k \trianglelefteq_{\mathsf{i}} R$ and $k \in \mathbb{N}$ that satisfies

$$\mathfrak{a}_0 M \subseteq \mathfrak{a}_1 M \subseteq \mathfrak{a}_2 M \subseteq \dots$$

there is some $s \in \mathbb{N}$ such that for any $i \in \mathbb{N}$ we get $\mathfrak{a}_{s+i} M = \mathfrak{a}_s M$, then M already is a noetherian R-module. The converse is true, as well, of course.

(3.120) Proposition: (viz. 909)
($\diamondsuit$) Let $(R, +, \cdot)$ be a commutative ring and L, M and N be R-modules, where L and M are artinian. Then the tensor product $L \otimes M$ is a module of finite length:

$$\ell\big(L \otimes M\big) < \infty$$

Let now $b : L \times M \to N$ be any bilinear map and pick up the notion of the *orthogonal complement* that will be introduced in (4.106), that is

$$\begin{aligned} L^{\top} &:= \{\, x \in M \mid \forall\, u \in L \,:\, b(u,x) = 0 \,\} \\ M^{\perp} &:= \{\, u \in L \mid \forall\, x \in M \,:\, b(u,x) = 0 \,\} \end{aligned}$$

If L and M are artinian, then the quotient modules $L/M^{\perp}$ and $M/L^{\top}$ are of finite length. In particular, if b is non-degenerate (i.e. $L^{\top} = 0$ and $M^{\perp} = 0$) then L and M are modules of finite length:

$$\ell\left(L \Big/ M^{\perp}\right) < \infty \quad \text{and} \quad \ell\left(M \Big/ L^{\top}\right) < \infty$$

3.12 Localization of Modules

We have already studied the localization of rings in section 2.10, now we would like to transfer this concept to modules. It turns out that the localization of modules combines neatly with the localization of rings. Also localization will preserve all the nice properites a module might have. Hence localization of modules is as powerful as the localization of rings and almost as useful.
Recall definition (2.113) which introduces the notion of a *multiplicatively closed* subset $U \subseteq R$ of a commutative ring $(R, +, \cdot)$. This is a subset U, such that $1 \in U$ and for any $u, v \in U$ we have $uv \in U$, as well. Also recall that a multiplicatively closed subset $U \subseteq R$ has been called *saturated* if $uv \in U$ implies $u \in U$ (and $v \in U$). We have already studied these sets in detail in section 2.10, so the reader is asked to refer to this section, in case of doubt. Let us now redo the construction of localization for modules in precisely the same manner, we used for rings:

(3.121) Definition: (viz. 1077)
Let $(R, +, \cdot)$ be any commutative ring, $U \subseteq R$ be a multiplicatively closed subset and M be an R-module. Then we obtain an equivalence relation $\sim$ on the set $U \times M$ by virtue of (with $x, y \in M$ and $u, v \in U$)

$$(u, x) \sim (v, y) \quad :\Longleftrightarrow \quad \exists\, w \in U \,:\, vwx = uwy$$

And we denote the quotient of $U \times M$ modulo $\sim$ by $U^{-1}M$ and the equivalence class of $(u, x) \in U \times M$ is denoted by x/u, formally we define

$$\begin{aligned} \frac{x}{u} &:= \{\, (v, y) \in U \times M \mid (u, x) \sim (v, y) \,\} \\ U^{-1}M &:= U \times M \Big/ \sim \end{aligned}$$

Now $U^{-1}M$ becomes an R-module again, even an $U^{-1}R$-module, under the following addition and scalar multiplications whith elements $a \in R$ and $a/u \in U^{-1}R$ respectively

$$\begin{aligned} \frac{x}{u} + \frac{y}{v} &:= \frac{vx + uy}{uv} \\ a\frac{x}{u} &:= \frac{ax}{u} \\ \frac{a}{u}\frac{y}{v} &:= \frac{ay}{uv} \end{aligned}$$

It is clear that under these operations the zero-element of $U^{-1}M$ is given to be $0/1$ and we obtain a canonical R-module homomorphism from M to $U^{-1}M$ by letting

$$\kappa \,:\, M \to U^{-1}M \,:\, x \mapsto \frac{x}{1}$$

In general this canonical homomorphism need not be and embedding (i.e. injective). Yet we do obtain the following implications for κ

$$\begin{aligned} U \subseteq \mathrm{NZD}_R(M) &\iff \kappa \text{ injective} \\ U \subseteq R^* &\implies \kappa \text{ bijective} \end{aligned}$$

(3.122) Remark: (viz. 1079)
The process of localization has already been commented on, in (2.117). However we would like to repeat some important properties of the localization. First of all x/u is zero, iff x can be annihilated by an element of U, that is

$$\frac{x}{u} = \frac{0}{1} \iff \exists\, w \in U : wx = 0$$

The next the important property is the cancellation of elements: Just as in the case of rings, the fractions x/u in $U^{-1}M$ can be reduced by common factors v of U. That is for any elements $x \in M$ and $u, v \in U$ we get the equality

$$\frac{vx}{vu} = \frac{x}{u}$$

And again this allows to express sums by going to a common denominator. That is consider $x_1, \ldots, x_n \in M$ and $u_1, \ldots, u_n \in U$. Then we denote $u := u_1 \ldots u_n \in U$ and $\widehat{u}_i := u/u_i \in U$ (e.g. $\widehat{u}_1 = u_2 \ldots u_n$). Then we have just noted that $x_i/u_i = (\widehat{u}_i x_i)/u$ and thereby

$$\frac{x_1}{u_1} + \cdots + \frac{x_n}{u_n} = \frac{\widehat{u}_1 x_1 + \cdots + \widehat{u}_n x_n}{u}$$

(3.123) Remark:
If $(R, +, \cdot)$ is a commutative ring, $U \subseteq R$ a multiplicatively closed set and A a commutative R-algebra, then the $U^{-1}R$-module $U^{-1}A$ also becomes an $U^{-1}R$-algebra, under the following multiplication

$$\cdot : U^{-1}A \times U^{-1}A \to U^{-1}A : \left(\frac{f}{u}, \frac{g}{u}\right) \mapsto \frac{fg}{uv}$$

Prob let us check that the multiplication is well-defined: Consider $f_1/u_1 = f_2/u_2$ and $g_1/v_1 = g_2/v_2$ and have to show $(f_1g_1)/(u_1v_1) = (f_2g_2)/(u_2v_2)$. By assumption there are some $p, q \in U$ such that $p\,u_2f_1 = p\,u_1f_2$ and $q\,v_2g_1 = q\,v_1g_2$. In particular $(pq)(u_2v_2)(f_1g_1) = (pu_2f_1)(qv_2g_1) = (pu_1f_2)(qv_1g_2) = (pq)(u_1v_1)f_2g_2$. But this is $(f_1g_1)/(u_1v_1) = (f_2g_2)/(u_2v_2)$. It is obvious, that this multiplication satisfies all the properties for $U^{-1}A$ to be an $U^{-1}R$-algebra. E.g. property (A) is just

$$\left(\frac{a}{w}\frac{f}{u}\right) \cdot \frac{g}{v} = \frac{(af) \cdot g}{w(uv)} = \frac{a(f \cdot g)}{w(uv)} = \frac{a}{w}\left(\frac{f}{u} \cdot \frac{g}{v}\right) = \frac{f \cdot (ag)}{u(wv)} = \frac{f}{u} \cdot \left(\frac{a}{w}\frac{g}{v}\right)$$

(3.124) Remark: (viz. 1079)
Let $(R, +, \cdot)$ be a commutative ring, $U \subseteq R$ be a multiplicatively closed set and let $S := U^{-1}R$. Now suppose M is an S-module already, then clearly M also is an R-module under the scalar multiplication

$$ax := \frac{a}{1}x$$

Let us emphasize this by writing M_R instead, if we consider M under this scalar multiplication with R. Under this construction we find:

(i) If we localize M_R in U we just find an isomorphic copy of M, to be explicit we have an isomorphism of S-modules the form

$$\kappa : M \xrightarrow{\sim} U^{-1}M_R : x \mapsto \frac{x}{1}$$

(ii) Also for any $u \in U$ we find that $\lambda_u : M_R \to M_R$ defined by scalar multiplication $\lambda_u(x) := ux$ is an automorphism of the R-module M_R.

(iii) And if N is another S-module and $\{ u/1 \mid u \in U \} \subseteq \text{NZD}_R(N)$ then a map $\varphi : M \to N$ is R-linear, if and only if it is S linear. In other words this is the equality

$$\text{mhom}(M_R, N_R) \quad = \quad \text{mhom}(M, N)$$

(3.125) Proposition: (viz. 1079)
Let $(R, +, \cdot)$ be a commutative ring $U \subseteq R$ be a multiplicatively closed set in R and let M be an R-module. Then the process of localization is compatible with sub-modules, homomorphsims, quotients and direct sums, in the following sense:

(i) If $P \leq_{\text{m}} M$ is an R-sub-module of M, then $U^{-1}P \leq_{\text{m}} U^{-1}M$ can be seen as an $U^{-1}R$-sub-module of $U^{-1}M$ canonically and we obtain the following isomorphy of $U^{-1}R$-modules

$$U^{-1}P \quad = \quad \left\{ \frac{x}{u} \mid x \in P, u \in U \right\} \quad \subseteq \quad U^{-1}M$$

$$U^{-1}\left(M \Big/ P \right) \quad \xrightarrow{\sim} \quad U^{-1}M \Big/ U^{-1}P \ : \ \frac{x+P}{u} \mapsto \frac{x}{u} + U^{-1}P$$

(ii) If N is another R-module and $\varphi : M \to N$ is a homomorphism of R-modules, then we obtain a homomorphism $U^{-1}\varphi$ of $U^{-1}R$-modules

$$U^{-1}\varphi \ : \ U^{-1}M \to U^{-1}N \ : \ \frac{x}{u} \mapsto \frac{\varphi(x)}{u}$$

And thereby $U^{-1}\varphi$ is injective, resp. surjective if and only if φ is injective, resp. surjective. In fact we even get the following identities

$$\begin{aligned} \text{kn}\left(U^{-1}\varphi \right) &= U^{-1}\text{kn}(\varphi) \\ \text{im}\left(U^{-1}\varphi \right) &= U^{-1}\text{im}(\varphi) \end{aligned}$$

(iii) If $I \neq \emptyset$ is an arbitrary index set and M_i is an R-module for any $i \in I$ then we obtain the following isomorphy of $U^{-1}R$-modules

$$\bigoplus_{i \in I} U^{-1}M_i \quad \xrightarrow{\sim} \quad U^{-1}\left(\bigoplus_{i \in I} M_i \right) \ : \ \left(\frac{x_i}{u_i} \right) \mapsto \frac{(\widehat{u}_i x_i)}{u}$$

Thereby u and $\widehat{u}_i$ are determined in the following way: Let $\Omega := \{ i \in I \mid x_i/u_i \neq 0/1 \}$ which is a finite set. In particular if I is finite itself we may simply take $\Omega = I$. Then $u := \prod_{i \in \Omega} u_i \in U$ is well-defined and for any $i \in I$ we let

$$\widehat{u}_i \quad := \quad \begin{cases} u/u_i \text{ if } i \in \Omega \\ \quad 1 \text{ if } i \notin \Omega \end{cases} \quad \in \quad U$$

(3.126) Remark: $(\diamondsuit)$
Suppose $(R,+,\cdot)$ is a commutative ring $U \subseteq R$ is multiplicatively closed and L, M and N are R-modules. If now $\varphi : L \to M$ and $\psi : M \to N$ are R-module homomorphisms then it is clear that

$$U^{-1}(\psi\psi) \;=\; (U^{-1}\psi)(U^{-1}\varphi)$$

As also $U^{-1}\mathbb{1} = \mathbb{1}$ this is a rather common situation that the more fancy language of category theory would put in the following way: The localization $M \mapsto U^{-1}M$ and $\varphi \mapsto U^{-1}\varphi$ is a covariant functor from the category of R-modules to the category of $U^{-1}R$-modules. Let us now regard a short exact sequence of R-modules, recall that the chain is said to be *exact* if at any position the image equals the kernel. In this case that is: φ is injective, ψ is surjective and $\mathrm{im}(\varphi) = \mathrm{kn}(\psi)$.

$$0 \to L \xrightarrow{\varphi} M \xrightarrow{\psi} N \to 0$$

Then the localization of this chain gives rise to the following short chain of $U^{-1}R$-modules. But then proposition (3.125.(ii)) implies that this localized chain is exact as well. In the fancy language of category theory again, that is: The localization functor $M \mapsto U^{-1}M$ and $\varphi \mapsto U^{-1}\varphi$ is *exact*.

$$0 \to U^{-1}L \xrightarrow{U^{-1}\varphi} U^{-1}M \xrightarrow{U^{-1}\psi} U^{-1}N \to 0$$

Prob as φ is injective, so is $U^{-1}\varphi$, since $\mathrm{kn}(U^{-1}\varphi) = U^{-1}\mathrm{kn}(\varphi) = U^{-1}0 = 0$. Likewise, as ψ is surjective, so is $U^{-1}\psi$, since $\mathrm{im}(U^{-1}\psi) = U^{-1}\mathrm{im}(\psi) = U^{-1}N$. And lastly we also find $\mathrm{im}(U^{-1}\varphi) = U^{-1}\mathrm{im}(\varphi) = U^{-1}\mathrm{kn}(\psi) = \mathrm{kn}(U^{-1}\psi)$. Altogether we found that the localized chain is exact again.

(3.127) Proposition: (viz. 1082)
Let $(R,+,\cdot)$ be a commutative ring and M be an R-module. If now $U \subseteq R$ is multiplicatively closed, then the sub-modules of the localization $U^{-1}M$ are selected from the sub-modules of M. That is we obtain an injective map

$$\overline{k} \;:\; \mathrm{Subm}_{U^{-1}R}(U^{-1}M) \hookrightarrow \mathrm{Subm}_R(M) \;:\; Z \mapsto \kappa^{-1}(Z)$$

$$\text{where} \quad \kappa^{-1}(Z) \;=\; \left\{ x \in M \mid \frac{x}{1} \in Z \right\}$$

This map $\overline{k}$ admits a left-inverse k (that is $k\overline{k} = \mathbb{1}$), that is surjective. And the left-inverse k is given by

$$k \;:\; \mathrm{Subm}_R(M) \twoheadrightarrow \mathrm{Subm}_{U^{-1}R}(U^{-1}M) \;:\; P \mapsto U^{-1}P$$

$$\text{where} \quad U^{-1}P \;=\; \left\{ \frac{x}{u} \mid x \in P \text{ and } u \in U \right\}$$

Thereby we generally get $P \subseteq \overline{k}k(P) = \{\, x \in M \mid \exists\, u \in U \,:\, ux \in P \,\}$ for any R-sub-module $P \leq_{\mathrm{m}} M$. And the converse inclusion is true if and only if P is pure, concerning elements the of U, this is to say

$$\overline{k}k(P) = P \quad\Longleftrightarrow\quad \forall\, x \in M \;\forall\, u \in U \,:\, ux \in P \implies x \in P$$

Both of these maps k and $\overline{k}$ are order preserving and respect intersections. That is for any sub-modules $P, Q \leq_{\mathsf{m}} M$ and $Y, Z, Z_i \leq_{\mathsf{m}} U^{-1}M$ we get

$$\begin{aligned} P \subseteq Q &\implies k(P) \subseteq k(Q) \\ Y \subseteq Z &\implies \overline{k}(Y) \subseteq \overline{k}(Z) \\ k(P \cap Q) &= k(P) \cap k(Q) \\ \overline{k}\left(\bigcap_{i\in I} Z_i\right) &= \bigcap_{i\in I} \overline{k}(Z_i) \end{aligned}$$

In particular, if we generalize k to arbitrary subsets $X \subseteq M$, i.e. for $k(X) := \{ x/u \mid x \in X, u \in U \}$, then we get the following equality of the sub-modules generated by X

$$\mathsf{Lh}_{U^{-1}R}\Big(k(X)\Big) = k\Big(\mathsf{Lh}_R(X)\Big)$$

(3.128) Remark:
It is clear that any $U^{-1}R$-sub-module of $U^{-1}M$ already is an R-sub-module of $U^{-1}M$. But the converse need not be true! That is an R-sub-module need not be an $U^{-1}R$-sub-module of $U^{-1}M$ and hence

$$\mathsf{Subm}_{U^{-1}R}(U^{-1}M) \subset \mathsf{Subm}_R(U^{-1}M)$$

As an example regard the localization $\mathbb{Z}$ in $2\mathbb{Z}$, that is we regard the $\mathbb{Z}$-module $\mathbb{Z}_{(2)} = (\mathbb{Z} \setminus 2\mathbb{Z})^{-1}\mathbb{Z}$ and consider it as a sub-module of $\mathbb{Z}_{(2)} = \{ a/2^k \mid a \in \mathbb{Z}, k \in \mathbb{N} \} \subseteq \mathbb{Q}$. Then it is clear that $\mathbb{Z} \subseteq \mathbb{Z}_{(2)}$ is an $\mathbb{Z}$-sub-module, but not an $\mathbb{Z}_{(2)}$-sub-module, as it is not an ideal.

Prob if Z is an $U^{-1}R$-sub-module then for any $x/u \in Z$ and any $a \in R$ we already get $a(x/u) = (ax)/u = (a/1)(x/u) \in Z$ again, hence the inclusion of sub-modules. And that $\mathbb{Z}$ is a $\mathbb{Z}$-sub-module of $\mathbb{Z}_{(2)}$ is clear (it is a commutative group under the addition), but it is not an ideal, since $(1/2)3 = 3/2 \notin \mathbb{Z}$.

(3.129) Remark:
Of course we could also generalize $\overline{k}$ to arbitrary subsets $W \subseteq U^{-1}M$, that is we could also denote $\overline{k}(W) := \{ x \in M \mid x/1 \in W \}$. However, $\overline{k}$ does not respect the generation of sub-modules, that is for an arbitrary subset $W \subseteq U^{-1}M$ it may occur that we only get one inclusion

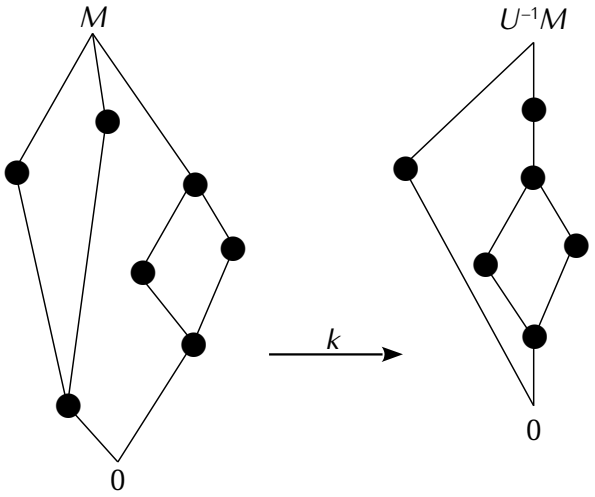
$$\mathsf{Lh}_R\Big(\overline{k}(W)\Big) \subset \overline{k}\Big(\mathsf{Lh}_{U^{-1}R}(W)\Big)$$

Prob let us first prove the inclusion "$\subseteq$": If $x \in \mathsf{Lh}_R(\overline{k}(W))$, then x is of the form $x = \sum_i a_i x_i$ where $x_i/1 \in W$. And we need to show that $x/1 \in \mathsf{Lh}_{U^{-1}R}(W)$ again. But this is easy, since

$$\frac{x}{1} = \sum_{i=1}^{n} \frac{a_i x_i}{1} = \sum_{i=1}^{n} \frac{a_i}{1}\frac{x_i}{1} \in \mathsf{Lh}_{U^{-1}R}(W)$$

As a counter-example to the equality regard $\mathbb{Z}_{(2)}$ again. If $W = \{ 1/2 \} \subseteq \mathbb{Z}_{(2)}$ then $\overline{k}(W)$ is empty, as $\overline{k}(W) = \{ x \in \mathbb{Z} \mid 2x = 1 \} = \emptyset$. Hence $\overline{k}(W)$ generates the sub-module $0 \leq_{\mathsf{m}} \mathbb{Z}$ of $\mathbb{Z}$. However W generates the entire $\mathbb{Z}_{(2)}$ as an $\mathbb{Z}_{(2)}$-sub-module. Hence $\overline{k}(\mathsf{Lh}_{\mathbb{Z}_{(2)}}(W)) = \overline{k}(\mathbb{Z}_{(2)}) = \mathbb{Z}$.

(3.130) Remark:
The following figure is supposed to enlighten the situation of the structure of sub-modules of $U^{-1}M$ a little: k is surjective, respects the inclusion and finite intersections. However if U contains an annihilator of P then $U^{-1}P = 0$ vanishes and hence it may well be the the structure of sub-modules will be reduced. Thus it may well occur that we get the following structure of sub-modules, where every sub-module is depicted as a $\bullet$:



(3.131) Corollary: (viz. 1096)
Let $(R, +, \cdot)$ be a commutative ring, $U \subseteq R$ be a multiplicatively closed subset and consider an R-module M. Regarding the localization $U^{-1}M$ as an $U^{-1}R$-module we get the following properties:

(i) If the set $\{ m_i \mid i \in I \} \subseteq M$ generates M as an R-module, then the set $\{ m_i/1 \mid i \in I \} \subseteq U^{-1}M$ generates $U^{-1}M$ as an $U^{-1}R$-module.

(ii) If the set $\{ m_i \mid i \in I \} \subseteq M$ is R-linearly independent, then the set $\{ m_i/1 \mid i \in I \} \subseteq U^{-1}M$ is $U^{-1}R$-linearly independent.

(iii) Consequentially: If the set $\{ m_i \mid i \in I \} \subseteq M$ is an R-basis of M, then $\{ m_i/1 \mid i \in I \} \subseteq U^{-1}M$ is an $U^{-1}R$-basis of $U^{-1}M$, as well.

(iv) If we abbreviate by $\star$ any one of the words *finitely generated*, *free*, *noetherian*, *artinian* or *injective*, then we get the following implication:

$$M \text{ is } \star \ R\text{-module} \quad \Longrightarrow \quad U^{-1}M \text{ is a } \star \ U^{-1}R\text{-module}$$

(3.132) Lemma: (viz. 1085) **Universal Property**
Let $(R, +, \cdot)$ and $(S, +, \cdot)$ be commutative rings, $U \subseteq R$ be multiplicatively closed and $\alpha : R \to S$ be a homomorphism of rings, such that $\alpha(U) \subseteq S^*$. Further consider an R-module M and an S-module N. Then N can be turned into both, an R and an $U^{-1}R$-module under the following scalar multiplications

$$R \times N \to N \ : \ (a, y) \mapsto ay := \alpha(a)y$$

$$U^{-1}R \times N \to N \ : \ (a/u, y) \mapsto \frac{a}{u}y := \alpha(u)^{-1}\alpha(a)y$$

If now $\varphi : M \to N$ is any R-module homomorphism, then there is a uniquely determined $U^{-1}R$-module homomorphism $\overline{\varphi} : U^{-1}M \to N$ such that $\varphi = \overline{\varphi}\kappa$. And this is given to be the following

$$\overline{\varphi} \ : \ U^{-1}M \to N \ : \ \frac{x}{u} \mapsto \alpha(u)^{-1}\varphi(x)$$

(3.133) Corollary: (viz. 1098)
Let $(R, +, \cdot)$ be any commutative ring and $U \subseteq R$ be multiplicatively closed. If further M and N are R-modules then the set $\mathrm{mhom}_R(M, N)$ of R-module homomorphisms from M to N is an R-module itself under the point-wise operations $(\varphi + \psi)(x) := \varphi(x) + \psi(x)$ and $(a\varphi)(x) := a\varphi(x)$. Hence we can even localize $\mathrm{mhom}_R(M, N)$ and thereby find the following homomorphism of R-modules

$$h \ : \ U^{-1}\mathrm{mhom}_R(M, N) \to \mathrm{mhom}_{U^{-1}R}(U^{-1}M, U^{-1}N) \ : \ \frac{\varphi}{u} \mapsto \frac{U^{-1}\varphi}{u}$$

Thereby $U^{-1}\varphi/u : U^{-1}M \to U^{-1}N$ is defined by $U^{-1}\varphi/u : x/v \mapsto \varphi(x)/uv$. And this homomorphism h even satisfies the following two additional properties:

(i) If M is finitely generated then h is injective.

(ii) If M admits a finite free presentation, then h is bijective. Nota a finite, free presentation of M is an exact chain of R-module homomorphisms of the form (where $m, n \in \mathbb{N}$)

$$R^m \xrightarrow{\alpha} R^n \xrightarrow{\omega} M \to 0$$

(3.134) Definition:
If $(R, +, \cdot)$ is a commutative ring and $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ is a prime ideal, then $R \setminus \mathfrak{p}$ is a multiplicatively closed (even saturated) set. Hence if M is an R-module we can define the localization of M with respect to this set. We will denote this localization by

$$M_{\mathfrak{p}} \ := \ (R \setminus \mathfrak{p})^{-1}M$$

Likewise if M and N are R-modules and $\varphi : M \to N$ is a homomorphism of R-modules, then we can localize φ as explained in (3.125.(ii))

$$\varphi_{\mathfrak{p}} \ : \ U^{-1}M \to U^{-1}N \ : \ \frac{x}{u} \mapsto \frac{\varphi(x)}{u}$$

(3.135) Lemma: (viz. 1097)
If $(R, +, \cdot)$ is any non-zero $R \neq 0$, commutative ring and M is an R-module, then the following three statements are equivalent

(a) $M = 0$

(b) $\forall\, \mathfrak{p} \in \mathrm{Spec}(R)$ we get $M_{\mathfrak{p}} = 0$

(c) $\forall\, \mathfrak{m} \in \mathrm{Smax}(R)$ we get $M_{\mathfrak{m}} = 0$

(3.136) Corollary: (viz. 1098)
If $(R,+,\cdot)$ is any non-zero $R \neq 0$, commutative ring, M is any R-module, $x \in M$ and $P \leq_{\mathfrak{m}} M$ is a sub-module of M. Then we get the equivaleny

$$x \in P \iff \forall\, \mathfrak{m} \in \mathrm{Smax}(R) \,:\, \frac{x}{1} \in P_{\mathfrak{m}}$$

(3.137) Corollary: (viz. 1098)
Let $(R,+,\cdot)$ be any non-zero $R \neq 0$, commutative ring, M and N be any R-modules and $\varphi : M \to N$ be an R-module homomorphism. If we now abbreviate by $\star$ any one of the words *injective*, *surjective*, *bijective* or *zero* (i.e. the zero homomorphism $x \mapsto 0$), then we obtain the following equivalences

(a) φ is $\star$

(b) $\forall\, \mathfrak{p} \in \mathrm{Spec}(R)$ we get $\varphi_{\mathfrak{p}}$ is $\star$

(c) $\forall\, \mathfrak{m} \in \mathrm{Smax}(R)$ we get $\varphi_{\mathfrak{m}} = 0$ is $\star$

(3.138) Definition:
Let $(R,+,\cdot)$ be a commutative ring and M be an R-module, then we define the **support** of M to be the collection of prime ideals $\mathfrak{p} \trianglelefteq_{\mathfrak{i}} R$ such that $M_{\mathfrak{p}} \neq 0$ is not the zero-module, that is

$$\mathrm{Supp}(M) \;:=\; \{\, \mathfrak{p} \in \mathrm{Spec}(R) \mid M_{\mathfrak{p}} \neq 0 \,\}$$

Remark: Note that by construction $M_{\mathfrak{p}} = 0$ is equivalent, to the following property: For any $x \in M$ there is some $u \in R \setminus \mathfrak{p}$ such that $ux = 0$. We will give equivalent constructions in (5.7.(iii)).

(3.139) Proposition: (viz. 1149)
Let $(R,+,\cdot)$ be a commutative ring, M and N be R-modules and consider $P \leq_{\mathfrak{m}} M$ a sub-module of M. Then we have the following statements

(i) The zero-module is the one and only R-module with empty support. That is we find the equivalence

$$M = 0 \iff \mathrm{Supp}(M) = \emptyset$$

(ii) There is an injective homomorphism of R-modules from M into the direct sum of the $M_{\mathfrak{p}}$ where $\mathfrak{p} \in \mathrm{Supp}(M)$ runs along the prime ideals of $\mathfrak{p} \trianglelefteq_{\mathfrak{i}} R$, that support M, given by

$$M \hookrightarrow \bigoplus_{\mathfrak{p} \in \mathrm{Supp}(M)} M_{\mathfrak{p}} \;:\; x \mapsto \left(\frac{x}{1}\right)$$

(iii) Recall the notation $\mathbb{V}(\mathfrak{a}) := \{\, \mathfrak{p} \subseteq \mathrm{Spec}(R) \mid \mathfrak{a} \subseteq \mathfrak{p} \,\}$ for some ideal $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$. If we regard $R/\mathfrak{a}$ as an R-module, then this equals the support of $R/\mathfrak{a}$

$$\mathrm{Supp}\left(R \Big/ \mathfrak{a}\right) \;=\; \mathbb{V}(\mathfrak{a})$$

(iv) Together the support of P and M/P build up the support of M, i.e. we find the following equality

$$\mathrm{Supp}(M) \;=\; \mathrm{Supp}(P) \cup \mathrm{Supp}\left(M \Big/ P\right)$$

More generally: If $0 \to L \to M \to N \to 0$ is a short exact chain of R-modules then the support of M combines the supports of both L and N, in formal terms

$$\mathrm{Supp}(M) \;=\; \mathrm{Supp}(L) \cup \mathrm{Supp}(N)$$

(v) Suppose $I \neq \emptyset$ is a non-empty index set and for any $i \in I$ we have a sub-module $P_i \leq_{\mathfrak{m}} M$. Then the support of the sum of the P_i is the union of the supports of the P_i, that is

$$\mathrm{Supp}\left(\sum_{i\in I} P_i\right) \;=\; \bigcup_{i\in I} \mathrm{Supp}(P_i)$$

(vi) If $M = \mathrm{Lh}\{\, m_i \mid i \in I \,\}$ (where $I \neq \emptyset$) and $\mathfrak{a}_i := \mathrm{ann}(m_i)$ is the annihilator of the element m_i then the support of M is given to be

$$\mathrm{Supp}(M) \;=\; \bigcup_{i\in I} \mathbb{V}(\mathfrak{a}_i)$$

In particular if M is finitely generated, then the support of M is the set of prime ideals of R that contain the annihilator of M

$$\mathrm{Supp}(M) \;=\; \mathbb{V}\big(\mathrm{ann}(M)\big)$$

More generally: If M is finitely generated and $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$ is an ideal of R, then the support of the R-module $M/\mathfrak{a}M$ is given to be

$$\mathrm{Supp}\left(M\big/_{\mathfrak{a}M}\right) \;=\; \mathbb{V}(\mathfrak{a}) \cap \mathbb{V}\big(\mathrm{ann}(M)\big) \;=\; \mathbb{V}\big(\mathfrak{a} + \mathrm{ann}(M)\big)$$

(vii) If M is finitely generated, then $a \in R$ is contained in all $\mathfrak{p} \in \mathrm{Supp}(M)$ if and only if the endomorphism $M \to M : x \mapsto ax$ is nilpotent. More explicitly this reads as

$$\bigcap \mathrm{Supp}(M) \;=\; \{\, a \in R \mid \exists\, n \in \mathbb{N} \,:\, a^n M = 0 \,\}$$

Now let $\mathfrak{a} \in R$ be an ideal of R, such that both M and $\mathfrak{a}$ are finitely generated. Then we find the following equivalence

$$\mathrm{Supp}(M) \;\subseteq\; \mathbb{V}(\mathfrak{a}) \quad\Longleftrightarrow\quad \exists\, n \in \mathbb{N} \,:\, \mathfrak{a}^n M = 0$$

(viii) $(\diamondsuit)$ If M and N are finitely generated, then the support of the tensor product $M \otimes N$ consists of those prime ideals $\mathfrak{p} \trianglelefteq_{\mathfrak{i}} R$, that support both M and N, that is

$$\mathrm{Supp}(M \otimes N) \;=\; \mathrm{Supp}(M) \cap \mathrm{Supp}(N)$$

In particular if both, M and N are finitely generated, then the tensor product $M \otimes N$ is zero if and only if there are a and $b \in R$, such that $a + b = 1$, $ax = 0$ for any $x \in M$ and $by = 0$ for any $y \in N$. In compact form this reads, as

$$M \otimes N \;=\; 0 \quad\Longleftrightarrow\quad \mathrm{ann}(M) + \mathrm{ann}(N) \;=\; R$$

3.13 Tensor Products

Consider some arbitrary, but non-empty, sets M_1, M_2 to M_n and denote their cartesian product by $X := M_1 \times \cdots \times M_n$. That is X consists of all n-tuples $(x_1, \ldots, x_n)$ where $x_j \in M_j$, formally

$$X \;=\; \{\, (x_1, \ldots, x_n) \mid \forall\, j \in 1 \ldots n \,:\, x_j \in M_j \,\}$$

And as all the M_j have been non-empty, so is X. Therefore, for any commutative ring $(R, +, \cdot)$, we can take a look at the free module $R^{\oplus X}$ generated by X over R. By definition this module consists of all sequences $a = (a_x) \in R^X$ indexed by $x \in X$, such that $a_x = 0$ for all but finitely many $x \in X$

$$R^{\oplus X} \;=\; \{\, a : X \to R : x \mapsto a_x \;\mid\; \#\{\, x \in X \mid a_x \neq 0 \,\} < \infty \,\}$$

As usual we write (a_x) instead of $a : x \mapsto a_x$ and take the addition and scalar-multiplication of $R^{\oplus X}$ to be point-wise: That is $b(a_x) = (ba_x)$ and $(a_x) + (b_x) = (a_x + b_x)$. And thereby we obtain the standard (Euclidean) basis $\{\, e_x \mid x \in X \,\}$ where $e_x : y \mapsto \delta_{x,y}$. That is $e_x : X \to R$ is the sequence with $e_x : x \mapsto 1$ and $e_x : y \mapsto 0$ for any other $y \neq x$. It stands to reason to identify $x \in X$ with e_x, i.e. we rewrite

$$\sum_{x \in X} a_x x \;:=\; \sum_{x \in X} a_x e_x \;=\; (a_x)$$

Note that this sum is well-defined, as $a_x = 0$ for all but *finitely* many $x \in X$. Using this notation the point-wise operations on $R^{\oplus X}$ take a particularly neat form

$$\begin{aligned} b \sum_{x \in X} a_x x \;&:=\; \sum_{x \in X} (b\, a_x) x \\ \sum_{x \in X} a_x x + \sum_{x \in X} b_x x \;&:=\; \sum_{x \in X} (b_x + a_x) x \end{aligned}$$

But what happens if the M_j are R-modules again, not only sets? The answer is rather deflating: Just nothing! Of course (for any $a \in R$ and any $x_i \in M_i$) the element $(ax_1, x_2, \ldots, x_n)$ is contained in $R^{\oplus X}$, but is has absolutely nothing to do with $a(x_1, x_2, \ldots, x_n)$. So in order to make the operations of $R^{\oplus X}$ compatible with the operations of the M_j we need to make certain identifications. To be precise we would like to have (for any $i \in 1 \ldots n$)

$$\begin{aligned} [x_1, \ldots, ax_i, \ldots, x_n] \;&=\; a\,[x_1, \ldots, x_i, \ldots, x_n] \\ [x_1, \ldots, x_i + y_i, \ldots, x_n] \;&=\; [x_1, \ldots, x_i, \ldots, x_n] + [x_1, \ldots, y_i, \ldots, x_n] \end{aligned}$$

where $[x_1, \ldots, x_n]$ denotes a suitable equivalence class of $(x_1, \ldots, x_n)$. This is the idea behind the following construction, so this is a completely natural thing to do. Thereby the equivalence class $[x_1, \ldots, x_n]$ will be $x_1 \otimes \ldots \otimes x_n$. However it is commonplace that - seeing this for the first time - this construction seems to be a little weird. The elements of $M_1 \otimes \ldots \otimes M_n$ are rather cumbersome to handle. In this sense the internal structure of $M_1 \otimes \ldots \otimes M_n$ worsens. But on the positive side the external structure of $M_1 \otimes \ldots \otimes M_n$ (i.e. how it interacts with other modules or constructions, like direct sums, localizations or homomorphisms) is extremely well-behaved. And this is precisely the reason, that gives this construction its powerful punch.

(3.140) Definition:
Let $(R,+,\cdot)$ be any commutative ring and consider some R-modules M_1 to M_n (where $1 \leq n \in \mathbb{N}$). First of all we take the cartesian product of the M_j as an index set, denoted by

$$X \;=\; M_1 \times \cdots \times M_n$$

Then we take to the free R-module $R^{\oplus X}$ generated by X over R and denote its Euclidean basis by $\{\, e_x \mid x \in X \,\}$, where $e_x : y \mapsto \delta_{x,y}$. Let us finally (for any $i \in 1 \ldots n$, $x = (x_1, \ldots, x_n) \in X$, $a \in R$ and $y_i \in M_i$) denote the following elements of $R^{\oplus X}$

$$\begin{aligned} s(i,x,a) &= a e_{(x_1,\ldots,x_i,\ldots,x_n)} - e_{(x_1,\ldots,ax_i,\ldots,x_n)} \\ a(i,x,y_i) &= e_{(x_1,\ldots,x_i,\ldots,x_n)} + e_{(x_1,\ldots,y_i,\ldots,x_n)} - e_{(x_1,\ldots,x_i+y_i,\ldots,x_n)} \end{aligned}$$

Then we denote the sub-module of $R^{\oplus X}$ generated by all these elements $s(i,x,a)$ and $a(i,x,y_i)$ by T

$$\begin{aligned} T \;:=\; & \mathrm{Lh}_R\{\, s(i,x,a) \mid i \in 1 \ldots n,\, x \in X,\, a \in R \,\} + \\ & \mathrm{Lh}_R\{\, a(i,x,y_i) \mid i \in 1 \ldots n,\, x \in X,\, y_i \in M_i \,\} \end{aligned}$$

Then we can finally define the **tensor product** $M_1 \otimes \ldots \otimes M_n$ of the M_j to be the quotient module of $R^{\oplus X}$ modulo this sub-module T. Also we define the **tensor product** $x_1 \otimes \ldots \otimes x_n$ of the elements $x_j \in M_j$ to be the equivalence class of $e_{(x_1,\ldots,x_n)}$, as an element of $M_1 \otimes \ldots \otimes M_n$

$$\begin{aligned} M_1 \otimes \ldots \otimes M_n &:= R^{\oplus X} \big/ T \\ x_1 \otimes \ldots \otimes x_n &:= e_{(x_1,\ldots,x_n)} + T \end{aligned}$$

(3.141) Remark:

(i) Let us explicitly give the generators of the sub-module T in case $n = 2$: The tensor product $M_1 \otimes M_2$ is the quotient of the free module $R^{\oplus(M_1 \times M_2)}$ by the sub-module T that is generated by the following elements, where x_1 and $y_1 \in M_1$ and x_2 and $y_2 \in M_2$ and $a \in R$

$$\begin{aligned} a e_{(x_1,x_2)} - e_{(ax_1,x_2)} \\ a e_{(x_1,x_2)} - e_{(x_1,ax_2)} \\ e_{(x_1,x_2)} + e_{(y_1,x_2)} - e_{(x_1+y_1,x_2)} \\ e_{(x_1,x_2)} + e_{(x_1,y_2)} - e_{(x_1,x_2+y_2)} \end{aligned}$$

(ii) By definition of the elements $s(i,x,a)$ and $a(i,x,y_i)$ it is clear that we get the following relations between these and the basis elements of $R^{\oplus X}$

$$\begin{aligned} e_{(x_1,\ldots,ax_i,\ldots,x_n)} + s(i,x,a) &= a e_{(x_1,\ldots,x_i,\ldots,x_n)} \\ e_{(x_1,\ldots,x_i+y_i,\ldots,x_n)} + a(i,x,y_i) &= e_{(x_1,\ldots,x_i,\ldots,x_n)} + e_{(x_1,\ldots,y_i,\ldots,x_n)} \end{aligned}$$

And as both $s(i,x,a)$ and $a(i,x,y_i)$ are contained in T they are eliminated when going to to the quotient. That is we immediately find the following relations in the tensor product $M_1 \otimes \ldots \otimes M_n$

$$\begin{aligned} x_1 \otimes \ldots \otimes (ax_i) \otimes \ldots \otimes x_n &= a(x_1 \otimes \ldots \otimes x_i \otimes \ldots \otimes x_n) \\ x_1 \otimes \ldots \otimes (x_i + y_i) \otimes \ldots \otimes x_n &= (x_1 \otimes \ldots \otimes x_i \otimes \ldots \otimes x_n) + \\ & \quad (x_1 \otimes \ldots \otimes y_i \otimes \ldots \otimes x_n) \end{aligned}$$

And this of course is precisely the reason for the construction of the tensor product. For more comments on our reasoning also refer to the introduction to this section. In other words these relations are nothing but the R-multi-linearity of the following map

$$\begin{aligned} \tau &: M_1 \times \cdots \times M_n \to M_1 \otimes \ldots \otimes M_n \\ &: (x_1, \ldots, x_n) \mapsto x_1 \otimes \ldots \otimes x_n \end{aligned}$$

(ii) Note that the first relation has a rather drastic consequence: If any element x_i of the tensor product $x_1 \otimes \ldots \otimes x_n$ is zero, then the entire tensor is zero

$$x_1 \otimes \ldots \otimes 0 \otimes \ldots \otimes x_n = 0 \otimes \ldots \otimes 0 \otimes \ldots \otimes 0 = 0$$

This is clear, as $0 \in M_i$ allows to pull $0 \in R$ out, annihilating the entire element $x_1 \otimes \ldots \otimes x_n$. This is the reason why we speak of the tensor *product*, in contrast to the direct *sum*, where a single zero does not annihilate the entire tuple $(x_1, \ldots, x_n)$. For more details on this refer to (3.154.(i)).

(iii) The converse need not be true, however. For example consider $1 \otimes 1 \in \mathbb{Z}_3 \otimes \mathbb{Z}_5$, then we have $1 \otimes 1 = 1 \otimes 6 = 3 \otimes 2 = 0 \otimes 2 = 0$. That is $x \otimes y = 0$ does *not* imply $x = 0$ or $y = 0$. In fact we have just seen, that the entire tensor product $\mathbb{Z}_3 \otimes \mathbb{Z}_5 = 0$ vanishes!

(iv) As the e_x generate $R^{\oplus X}$ (they even form an R-basis) it is clear that the elements $x_1 \otimes \ldots \otimes x_n$ generate the tensor product $M_1 \otimes \ldots \otimes M_n$. That is every element of the tensor-product can be written (in a non-unique way!) as (for some $a_k \in R$ and $x_{i,k} \in M_i$)

$$\sum_{k=1}^{m} a_k (x_{1,k} \otimes \ldots \otimes x_{n,k})$$

(v) Consider any tensor $t \in M_1 \otimes \ldots \otimes M_n$ then we define the **rank** $\mu(t)$ of t to be the minimal number of *pure* tensors $x_{1,k} \otimes \ldots \otimes x_{n,k}$ which are required to build up t

$$\mu(t) := \min \left\{ m \in \mathbb{N} \;\middle|\; \begin{array}{l} \exists\, a_k \in R \\ \exists\, x_{i,k} \in M_k \end{array} : t = \sum_{k=1}^{m} a_k\, x_{1,k} \otimes \ldots \otimes x_{n,k} \right\}$$

(vi) On some rare occasions we use more than one ring R. In this case we emphasize the ring R used for the construction (that is R in the free module $R^{\oplus X}$) of the tensor product, by writing

$$M_1 \otimes_R \ldots \otimes_R M_n := M_1 \otimes \ldots \otimes M_n$$

(vii) For simplicities sake we have used a commutative base ring R here. However it is possible to define the tensor product over non-commutative rings, as well. The complication is, in case of non-commutative rings the scalar multiplication from the right yields a different result. Hence in this case one has to introduce the notion of *R-S-bimodules* first, an approach followed e.g. in the highly recommended textbook of [Adkins, Weintraub, Algebra, GTM 136].

Let us now consider the R-modules M_1 to M_n over a fixed commutative ring $(R, +, \cdot)$ again. If now N is another R-module, then recall that a map $\varphi : M_1 \times \cdots \times M_n \to N$ has been said to be *R-multilinear*, iff for any $i \in 1 \dots n$ and any fixed $x_j \in M_j$ [where $i \neq j \in 1 \dots n$] the maps

$$M_i \to N \ : \ x_i \mapsto \varphi(x_1, \dots, x_i, \dots, x_n)$$

are R-linear (that is homomorphisms of R-modules) - see the end of section 3.8 for a more detailed definition of this notion. And as we have seen in the remark above that the map

$$\tau \ : \ M_1 \times \cdots \times M_n \to M_1 \otimes \dots \otimes M_n \ : \ (x_1, \dots, x_n) \mapsto x_1 \otimes \dots \otimes x_n$$

is R-multilinear. In fact if φ is *any* R-multilinear map, as above, then φ already factors through τ, that is $\varphi = \overline{\varphi}\tau$ for some R-linear map $\overline{\varphi}$. This is the so-called *universal property* of the tensor product:

(3.142) Lemma: (viz. 1118)
Let $(R, +, \cdot)$ be any commutative ring and consider the R-modules M_1 to M_n (where $1 \leq n \in \mathbb{N}$) and N. If now φ is any R-multilinear map

$$\varphi \ : \ M_1 \times \cdots \times M_n \to N$$

then φ factors through $\tau : (x_1, \dots, x_n) \mapsto x_1 \otimes \dots \otimes x_n$, that is there is a uniquely determined R-linear map $\overline{\varphi}$ such that $\varphi = \overline{\varphi}\tau$ and thereby

$$\begin{aligned} \overline{\varphi} \ &: \ M_1 \otimes \dots \otimes M_n \to N \\ &: \ \sum_{i=1}^{k} a_i (x_{i,1} \otimes \dots \otimes x_{i,n}) \mapsto \sum_{i=1}^{k} a_i \varphi(x_{i,1}, \dots, x_{i,n}) \end{aligned}$$

Thereby the map $\varphi \mapsto \overline{\varphi}$ is an isomorphism of R-modules from the R-multilinear maps on $M_1 \times \cdots \times M_n$ to the R-linear maps on $M_1 \otimes \dots \otimes M_n$

$$\mathrm{mult}_R(M_1 \times \cdots \times M_n, N) \ \xrightarrow{\sim} \ \mathrm{mhom}_R(M_1 \otimes \dots \otimes M_n, N) \ : \ \varphi \mapsto \overline{\varphi}$$

(3.143) Remark:
Let R be a commutative ring and L, M and N be R-modules again. Note that a map $\varphi : L \times M \to N$ is bilinear if and only if its stepwise iteration $L \to \mathrm{mhom}(M, N) : \ell \mapsto (m \mapsto \varphi(\ell, m))$ is linear. Hence we can identify the multi-linear maps $L \times M \to N$ with $\mathrm{mhom}(L, \mathrm{mhom}(M, N))$ and thereby find the following isomorphies of R-modules

$$\begin{array}{rcl} \mathrm{mhom}(L \otimes M, N) & \xrightarrow{\sim} & \mathrm{mhom}(L, \mathrm{mhom}(M, N)) \\ \varphi & \mapsto & (\ell \mapsto (m \mapsto \varphi(\ell \otimes m))) \\ \mathrm{mhom}(L \otimes M, N) & \xrightarrow{\sim} & \mathrm{mhom}(M, \mathrm{mhom}(L, N)) \\ \varphi & \mapsto & (m \mapsto (\ell \mapsto \varphi(\ell \otimes m))) \end{array}$$

(3.144) Corollary: (viz. 1119)
Let $(R, +, \cdot)$ be a commutative ring and M_1 to M_n be R-modules. Then the tensor product of these modules is associative and commutative up to isomorphy. That is we get the following isomorphies:

(i) If $\sigma \in S_n$ is any permutation of $1 \ldots n$, then we find the following isomorphy of the R-modules $M_1 \otimes \ldots \otimes M_n$ and $M_{\sigma(1)} \otimes \ldots \otimes M_{\sigma(n)}$

$$\begin{array}{rcl} M_1 \otimes \ldots \otimes M_n & \xrightarrow{\sim} & M_{\sigma(1)} \otimes \ldots \otimes M_{\sigma(n)} \\ \sum_{k=1}^{m} a_k \, x_{1,k} \otimes \ldots \otimes x_{n,k} & \mapsto & \sum_{k=1}^{m} a_k \, x_{\sigma(1),k} \otimes \ldots \otimes x_{\sigma(n),k} \end{array}$$

(ii) Suppose $I(1)$ to $I(s)$ are a partition of the set $1 \ldots n$, that is the $I(j)$ are pairwise disjoint [that is $j \neq k \implies I(j) \cap I(k) = \emptyset$ and also $I(1) \cup \cdots \cup I(s) = 1 \ldots n$]. Let $r(j) := \#I(j)$ and say $I(j)$ is given to be $I(j) = \{ i(j,1), \ldots, i(j, r(j)) \}$ for any $j \in 1 \ldots s$. Then we may rearrange the indexes $j \in 1 \ldots n$ arbitrarily and still find the following isomorphy of R-modules

$$\begin{array}{rcl} \bigotimes_{i=1}^{n} M_i & \xrightarrow{\sim} & \bigotimes_{j=1}^{s} \left(\bigotimes_{k=1}^{r(j)} M_{i(j,k)} \right) \\ \sum_{k=1}^{m} a_m \, x_{1,k} \otimes \ldots \otimes x_{n,k} & \mapsto & \sum_{k=1}^{m} a_k \, \otimes_{j=1}^{s} \left(\otimes_{k=1}^{r(j)} x_{i(j,k),k} \right) \end{array}$$

In particular, if L, M and N are R-modules then the tensor product is associative, up to isomorphy. That is the find the isomorphy of the R-modules $L \otimes (M \otimes N)$ and $(L \otimes M) \otimes N$, via:

$$\begin{array}{rcl} L \otimes (M \otimes N) & \xrightarrow{\sim} & (L \otimes M) \otimes N \\ \sum_{k=1}^{m} a_k \, x_k \otimes (y_k \otimes z_k) & \mapsto & \sum_{k=1}^{m} a_k \, (x_k \otimes y_k) \otimes z_k \end{array}$$

(iii) If A_1 to A_n even are R-(semi-)algebras, then the tensor product of these $A_1 \otimes \ldots \otimes A_n$ is an R-(semi-)algebra as well, where the multiplication is taken to be the following

$$\begin{array}{rcl} \left(\sum_{j=1}^{\ell} a_j \, x_{1,j} \otimes \ldots \otimes x_{n,j} \right) \cdot \left(\sum_{k=1}^{m} b_k \, y_{1,k} \otimes \ldots \otimes y_{n,k} \right) & & \\ := & \left(\sum_{j=1}^{\ell} \sum_{k=1}^{m} a_j \, b_k \, (x_{1,j} y_{1,k}) \otimes \ldots \otimes (x_{n,j} y_{n,k}) \right) & \end{array}$$

(3.145) Corollary: (viz. 1122)
Let $(R,+,\cdot)$ be a commutative ring and for any $i \in 1\ldots n$ consider an R-algebra A_i whose unit element we denote by $1_i \in A_i$. For any $x_1 \in A_1$ let us denote $\overline{x}_1 = x_1 \otimes 1_2 \otimes \ldots \otimes 1_n$ and so on, up to $\overline{x}_n = 1_1 \otimes \ldots \otimes 1_{n-1} \otimes x_n$ for some $x_n \in A_n$ That is $\overline{x}_j = \iota_j(x_j)$ where ι_j is the R-algebra-homomorphism

$$\iota_j \;:\; A_j \to \bigotimes_{i=1}^{n} A_i \;:\; x_j \mapsto \bigotimes_{i=1}^{n} \begin{cases} x_j \text{ if } i = j \\ 1_i \text{ if } i \neq j \end{cases}$$

Now let B be another R-semi-algebra and consider some R-algebra-homomorphisms $\alpha_i : A_i \to B$ such that for any $i \in 1\ldots n$ we have $\mathrm{im}(\alpha_i) \subseteq \mathrm{CEN}(B)$. Then there is a uniquely determined R-algebra-homomorphism

$$\overline{\alpha} \;:\; A_1 \otimes \ldots \otimes A_n \to B$$

such that for all $j \in 1\ldots n$ we get $\overline{\alpha}\iota_j = \alpha_j$ (that is $\overline{\alpha}(\overline{x}_j) = \alpha_j(x_j)$ for any $x_j \in A_j$). And this is explicitly given to be the following

$$\overline{\alpha}\left(\sum_{k=1}^{m} a_k\, x_{1,k} \otimes \ldots \otimes x_{n,k}\right) \;=\; \sum_{k=1}^{m} a_k\, \alpha_1(x_{1,k}) \cdot \cdots \cdot \alpha_n(x_{n,k})$$

(3.146) Proposition: (viz. 1122)
Let $(R,+,\cdot)$ be a commutative ring and consider the R-modules M and N. Then we study the result of applying the tensor product in the standard-cases:

(i) We obtain an isomorphy between $R \otimes M$ and M, as given below. In this sense the base ring R is the unit element of the tensor product

$$\begin{array}{rcl} R \otimes M & \xrightarrow{\sim} & M \\ \sum_{k=1}^{m} a_k \otimes x_k & \mapsto & \sum_{k=1}^{m} a_k x_k \end{array}$$

(ii) If $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ is an ideal in R, then the quotient ring $R/\mathfrak{a}$ is an R-module under the scalar multiplication $a(b+\mathfrak{a}) = ab + \mathfrak{a}$. And taking to the tensor product we find the following isomorphy of R-modules

$$\begin{array}{rcl} R\big/_{\mathfrak{a}} \otimes M & \xrightarrow{\sim} & M\big/_{\mathfrak{a}M} \\ \sum_{k=1}^{m} a_k\,(b_k+\mathfrak{a}) \otimes x_k & \mapsto & \sum_{k=1}^{m} a_k b_k x_k + \mathfrak{a}M \end{array}$$

(iii) If $\mathfrak{a}$ and $\mathfrak{b} \trianglelefteq_{\mathrm{i}} R$ are two ideals of R, then any element of the tensor product $(R/\mathfrak{a}) \otimes (R/\mathfrak{b})$ can be written in the form $(1+\mathfrak{a}) \otimes (r+\mathfrak{b})$ for some $r \in R$. And thereby we obtain an isomorphism of R-modules of the following form

$$\begin{array}{rcl} R\big/_{\mathfrak{a}} \otimes R\big/_{\mathfrak{b}} & \xrightarrow{\sim} & R\big/_{\mathfrak{a}+\mathfrak{b}} \\ (r+\mathfrak{a}) \otimes (s+\mathfrak{b}) & \mapsto & rs + (\mathfrak{a}+\mathfrak{b}) \end{array}$$

In particular (for $\mathfrak{a} = 0$ and $\mathfrak{b} = 0$) we obtain a very peculiar isomorphy of R to its tensor product $R \otimes R$ by virtue of the following map

$$R \otimes R \quad \xrightarrow{\sim} \quad R \;:\; a \otimes b \mapsto ab$$

(iv) Likewise, if $U \subseteq R$ is a multiplicatively closed set, then the localization $U^{-1}R$ is an R-module under the scalar multiplication $a(b/u) = (ab)/u$. And this time we find the following isomorphy of R-modules

$$\begin{array}{ccc} U^{-1}R \otimes M & \xrightarrow{\sim} & U^{-1}M \\ \displaystyle\sum_{k=1}^{m} a_k \, \frac{b_k}{u_k} \otimes x_k & \mapsto & \displaystyle\sum_{k=1}^{m} \frac{a_k b_k x_k}{u_k} \end{array}$$

(v) If M is a free module, then $M \otimes N$ is isomorphic to $\dim(M)$ copies of N. That is: If $\{ m_i \mid i \in I \}$ is an R-basis of M, then we obtain an isomorphism of the following R-modules

$$\begin{array}{ccc} N^{\oplus I} & \xrightarrow{\sim} & M \otimes N \\ (y_i) & \mapsto & \displaystyle\sum_{i \in I} m_i \otimes y_i \end{array}$$

(vi) If M and N both are free R-modules with the bases $\{ m_i \mid i \in I \}$ and $\{ n_j \mid j \in J \}$ respectively, then $M \otimes N$ is a free R-module with basis $\{ m_i \otimes n_j \mid i \in I, j \in J \}$. In particular we get

$$\dim(M \otimes N) \quad = \quad \dim(M) \cdot \dim(N)$$

And by induction it is clear, that if $M_1, \ldots, M_n$ are free R-modules with the bases $\{ m_{i,j} \mid i \in I(j) \}$ (where $j \in 1 \ldots n$) respectively, then the tensor product $M_1 \otimes \ldots \otimes M_n$ is a free R-module with the basis $\left\{ m_{i(1),1} \otimes \ldots \otimes m_{i(n),n} \mid i(1) \in I(1), \ldots, i(n) \in I(n) \right\}$.

(vii) The tensor product is compatible with direct sums: That is, if M_i (for $i \in I$) and N_j (for $j \in J$) are families of R-modules, then we obtain the following isomorphy of R-modules

$$\begin{array}{ccc} \left(\displaystyle\bigoplus_{i \in I} M_i \right) \otimes \left(\displaystyle\bigoplus_{j \in J} N_j \right) & \xrightarrow{\sim} & \displaystyle\bigoplus_{(i,j) \in I \times J} M_i \otimes N_j \\ \displaystyle\sum_{k=1}^{m} a_k (x_{i,k}) \otimes (y_{i,k}) & \mapsto & \displaystyle\sum_{k=1}^{m} a_k (x_{i,k} \otimes y_{j,k}) \end{array}$$

(viii) ($\diamondsuit$) Let A and B be commutative monoids and regard the polynomial rings $R[s \mid A]$ and $R[t \mid B]$ as R-algebras. Then $A \times B$ is a commutative monoid again such that we may also form the R-algebra $R[x \mid A \times B]$. And thereby we find that $R[x \mid A \times B]$ is nothing the tensor product of $R[s \mid A]$ and $R[t \mid B]$. That is we find the isomorphism of R-algebras

$$\begin{array}{ccc} R\left[x \mid A \times B\right] & \xrightarrow{\sim} & R\left[s \mid A\right] \otimes R\left[t \mid B\right] \\ \displaystyle\sum_{(\alpha,\beta) \in A \times B} f\left[\alpha, \beta\right] \, x^{(\alpha,\beta)} & \mapsto & \displaystyle\sum_{(\alpha,\beta) \in A \times B} f\left[\alpha, \beta\right] \, s^{\alpha} \otimes t^{\beta} \end{array}$$

And if A_1 to A_n are commutative monoids, then by induction on n it is clear that this generalizes to the following isomorphy of R-algebras

$$R[x \mid A_1 \times \cdots \times A_n] \quad \cong_{\mathsf{a}} \quad R[t \mid A_1] \otimes \ldots \otimes R[t \mid A_1]$$

(3.147) Remark:
Let us take a closer look at (3.146.(v)): As the elements of $N^{\oplus I}$ are of the form (y_i) where $y_i = 0$ for all but finitely many $i \in I$, we find that the elements of $t \in M \otimes N$ are of the form

$$t \quad \in \quad \sum_{i \in I} m_i \otimes y_i$$

where $\#\{\, i \in I \mid y_i \neq 0 \,\} < \infty$ again. In fact this representation of an element of $M \otimes N$ is *unique*. As $y = (y_i)$ and $y' = (y'_i)$ are equal $y = y'$ if an only if we have $y_i = y'_i$ for any $i \in I$ this property is transferred to $M \otimes N$. That is in $M \otimes N$ we find the equivalence of

$$\sum_{i \in I} m_i \otimes y_i \;=\; \sum_{i \in I} m_i \otimes y'_i \quad \Longleftrightarrow \quad \forall\, i \in I \;:\; y_i = y'_i$$

(3.148) Definition:
Let $(R, +, \cdot)$ be a commutative ring and let $\varphi_i : M_i \to N_i$ (where $i \in 1 \ldots n$) be R-module homomorphisms between the R-modules M_i and N_i. Then we obtain an R-multi-linear map, by letting

$$\begin{aligned} \varphi_1 \times \cdots \times \varphi_n \quad &: \quad M_1 \times \cdots \times M_n \to N_1 \otimes \ldots \otimes N_n \\ &: \quad (x_1, \ldots, x_n) \mapsto \varphi(x_1) \otimes \ldots \otimes \varphi(x_n) \end{aligned}$$

And according to the universal property (3.142) this induces an R-linear map, which we denote by $\varphi_1 \otimes \ldots \otimes \varphi_n := \overline{\varphi_1 \times \cdots \times \varphi_n}$ and which is explicitly given to be

$$\begin{aligned} \varphi_1 \otimes \ldots \otimes \varphi_n \quad &: \quad M_1 \otimes \ldots \otimes M_n \to N_1 \otimes \ldots \otimes N_n \\ &: \quad \sum_{k=1}^{m} a_k\, x_{1,k} \otimes \ldots \otimes x_{n,k} \mapsto \sum_{k=1}^{m} a_k\, \varphi_1(x_{1,k}) \otimes \ldots \otimes \varphi_n(x_{n,k}) \end{aligned}$$

This map is called the **tensor product** of the φ_i. It is common practice that in case of φ_i being the identity map $\varphi_i = \mathbb{1}_i : M_i \to N_i = M_i : x \mapsto x$ we will just write $\varphi_1 \otimes \ldots \otimes M_i \otimes \ldots \otimes \varphi_n$, instead of $\varphi_1 \otimes \ldots \otimes \mathbb{1}_i \otimes \ldots \otimes \varphi_n$.

(3.149) Lemma: (viz. 1128)
Let $(R, +, \cdot)$ be a commutative ring and let $\varphi_i : L_i \to M_i$ and $\psi_i : M_i \to N_i$ (where $i \in 1 \ldots n$) be R-module homomorphisms between the R-modules L_i and M_i and N_i respectively.

(i) Let $\mathbb{1}_i : M_i \to M_i : x \mapsto x$ be the identity map on M_i. Then the tensor product of the $\mathbb{1}_i$ is the identity map on $M_1 \otimes \ldots \otimes M_n$, formally that is

$$\mathbb{1}_1 \otimes \ldots \otimes \mathbb{1}_n \;=\; \mathbb{1}_{M_1 \otimes \ldots \otimes M_n} \;:\; t \mapsto t$$

(ii) The tensor product of homomorphisms is compatible with the composition of maps, which is to say

$$\left(\bigotimes_{i=1}^{n}\psi_i\right)\left(\bigotimes_{i=1}^{n}\varphi_i\right) \;=\; \bigotimes_{i=1}^{n}(\psi_i\varphi_i)$$

(iii) If all the φ_i are surjective (respectively bijective), then the tensor product $\otimes_{i=1}^{n}\varphi_i$ is surjective (respectively bijective) again. And in case R is a field we also get: If all the φ_i are injective, then the tensor product $\otimes_{i=1}^{n}\varphi_i$ is injective again.

(iv) In case R is an arbitrary commutative ring we still get: If for any $i \in 1\ldots n$ we have that (1) φ_i is injective and (2) there is some sub-module $P_i \leq_{\mathfrak{m}} M_i$ such that $\mathrm{im}(\varphi_i) \oplus P_i = M_i$ then we get that (a) $\varphi_1 \otimes \ldots \otimes \varphi_n$ is injective and (b) there is some sub-module $P \leq_{\mathfrak{m}} M_1 \otimes \ldots \otimes M_n$ such that

$$M_1 \otimes \ldots \otimes M_n \;=\; \mathrm{im}(\varphi_1 \otimes \ldots \otimes \varphi_n) \oplus P$$

(3.150) Remark:
Consider the R-modules M, M' and N over the commutative ring $(R,+,\cdot)$ and suppose $\Phi : M \xrightarrow{\sim} M'$ is an isomorphism. Then by (3.149.(iii)) $\Phi \otimes \mathbb{1}_N$ is an isomorphism, as well. And it is of the form

$$M \otimes N \;\xrightarrow{\sim}\; M' \otimes N \;:\; \sum_{k=1}^{m} a_k\, x_k \otimes y_k \mapsto \sum_{k=1}^{m} a_k\, \Phi(x_k) \otimes y_k$$

Therefore any isomorphy of modules is preserved if we append another module using a tensor product. We will use this property to prove the following statements:

(3.151) Corollary: (viz. 1129)
Let $(R,+,\cdot)$ be a commutative ring, $U \subseteq R$ be a multiplicatively closed set and denote $S := U^{-1}R$. If now M and N are two R-modules, then we obtain the following isomorphies

(i) If we regard $U^{-1}M$ and $U^{-1}N$ as R-modules again, then we obtain an isomorphism of R-modules that is defined by linear expansion of

$$\begin{array}{ccc} U^{-1}M \otimes U^{-1}N & \xrightarrow{\sim} & U^{-1}(M \otimes N) \\ \frac{x}{u} \otimes \frac{y}{v} & \mapsto & \frac{x \otimes y}{uv} \end{array}$$

(ii) By construction $U^{-1}M$ and $U^{-1}N$ are S-modules, but we can also regard these as R-modules. We denote this by using the index R, as in (3.124). Then we find the following isomorphy of R-modules

$$\begin{array}{ccc} \left(U^{-1}M\right)_R \otimes_R \left(U^{-1}N\right)_R & \xrightarrow{\sim} & \left(U^{-1}M \otimes_S U^{-1}N\right)_R \\ \frac{x}{u} \otimes_R \frac{y}{v} & \mapsto & \frac{x}{u} \otimes_S \frac{y}{v} \end{array}$$

(3.152) Remark: (viz. 1133)
Kronecker Product: Let $(R,+,\cdot)$ be a commutative ring and $\varphi : M \to N$ and $\psi : U \to V$ be homomorphisms between the R-modules M, N, U and V. Suppose all these modules are finitely generated, free and let us denote the bases of these by $\mathcal{M} = \{ m_j \mid j \in 1 \dots n \}$ of M, $\mathcal{N} = \{ n_i \mid i \in 1 \dots m \}$ of N, $\mathcal{U} = \{ u_l \mid l \in 1 \dots q \}$ of U and finally $\mathcal{V} = \{ v_k \mid k \in 1 \dots p \}$ of V. Also let $[\varphi] = A = (a_{i,j}) \in \mathrm{mat}_{m,n}(R)$ and $[\psi] = B = (b_{k,l}) \in \mathrm{mat}_{p,q}(R)$ be the matrix representations of φ and ψ respectively. That is we have

$$\varphi(m_j) \;=\; \sum_{i=1}^{m} a_{i,j} n_i \quad \text{and} \quad \psi(u_l) \;=\; \sum_{k=1}^{p} b_{k,l} v_k$$

By (3.146.(v)) $M \otimes U$ inherits the basis $\{ m_j \otimes u_l \mid (j,l) \in (1 \dots n) \times (1 \dots q) \}$ and in particular is a free $(n \cdot q)$-dimensional module. Likewise $N \otimes V$ is a free $(m \cdot p)$-dimensional module, as it features the basis $\{ n_i \otimes v_k \mid (i,k) \in (1 \dots m) \times (1 \dots p) \}$. Due to the multi-linearity of the tensor product we find

$$(\varphi \otimes \psi)(m_j \otimes u_l) \;=\; \varphi(m_j) \otimes \psi(u_l) \;=\; \sum_{i=1}^{m} \sum_{k=1}^{p} a_{i,j} b_{k,l}\, n_i \otimes v_k$$

From this we find the matrix representation of $\varphi \otimes \psi : M \otimes U \to N \otimes V$ to be composed of the products $a_{i,j} b_{k,l}$ of the coefficients of A and B, that is

$$[\varphi \otimes \psi]_{(i,k),(j,l)} \;=\; a_{i,j} b_{k,l} \;=\; [\varphi]_{i,j}\, [\psi]_{k,l}$$

We need to order the bases of $M \otimes U$ and $N \otimes V$ to fix a matrix representation of $\varphi \otimes \psi$. So we install the lexicographic order $(1,1) < (1,2) < \dots < (1,p) < (2,1) < \dots < (m,p)$. That is $(i,k) = p(i-1)+k \in 1 \dots mp$ and $(j,l) = q(j-1)+l \in 1 \dots nq$. It stands to reason to denote this so called **kronecker product** of the matrices A and B by $A \otimes B$ again. That is we define $A \otimes B \in \mathrm{mat}_{mp,nq}(R)$ to be $[A \otimes B]_{(i,k),(j,l)} := [A]_{i,j} \cdot [B]_{k,l} \in R$. In block form this reads as

$$A \otimes B \;=\; \begin{pmatrix} a_{1,1}B & \cdots & a_{1,n}B \\ \vdots & & \vdots \\ a_{m,1}B & \cdots & a_{m,n}B \end{pmatrix}$$

e.g.

$$\begin{pmatrix} 0 & 1 & 0 \\ 2 & 0 & 3 \\ 0 & 4 & 0 \end{pmatrix} \otimes \begin{pmatrix} a & 2 \\ 0 & 1 \end{pmatrix} \;=\; \begin{pmatrix} 0 & 0 & a & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 2a & 4 & 0 & 0 & 3a & 6 \\ 0 & 2 & 0 & 0 & 0 & 3 \\ 0 & 0 & 4a & 8 & 0 & 0 \\ 0 & 0 & 0 & 4 & 0 & 0 \end{pmatrix}$$

Recall that we defined the kronecker product of two matrices in precisely that way, as to ensure the following equality of matrix representations:

$$[\varphi \otimes \psi] \;=\; [\varphi] \otimes [\psi]$$

And using (3.149) or direct computations, it is clear, that the kronecker product features the properties

$$\begin{aligned}
\mathbb{1}_m \otimes \mathbb{1}_n &= \mathbb{1}_{mn} \\
A \otimes B &= (A \otimes \mathbb{1}_p)(\mathbb{1}_n \otimes B) \\
A \otimes (bB + D) &= b(A \otimes B) + (A \otimes D) \\
(aA + C) \otimes B &= a(A \otimes B) + (C \otimes B) \\
(A \otimes B)^* &= A^* \otimes B^* \\
(A \otimes B)(C \otimes D) &= (AC) \otimes (BD) \\
\mathrm{tr}(A \otimes B) &= \mathrm{tr}(A) \cdot \mathrm{tr}(B)
\end{aligned}$$

After these all these examples it should be understood, that the tensor product is very well-behaved and highly compatible with all the different constructions we employed so far. That is the *external* structure of tensor products is immaculate indeed.
But looking at the proofs we see that all these properties have been derived by constructing the required isomorphisms using the universal property. We rarely employed computations with tensor elements. This is due to the sad fact that the *internal* structure of the tensor product is very hard to control: Lots of weird things can happen if we look at the tensor elements directly, as T is hard to control directly. However dealing with free modules the internal structure of the tensor product is well domesticated, as well. To get a glimpse of this compare (3.153) to (3.154.(i)).

(3.153) Proposition: (viz. 1148)
Let $(R, +, \cdot)$ be a commutative ring, M and N be R-modules. Suppose we are given a generating set of $N = \mathrm{Lh}\{ n_j \mid j \in J \}$ and a family of elements $\{ m_j \mid j \in J \} \subseteq M$ such that only finitely many m_j are non-zero [that is $\#\{ j \in J \mid m_j \neq 0 \} < \infty$]. Then

$$\sum_{j \in J} m_j \otimes n_j = 0$$

is zero, if and only if there are some elements x_1 to $x_m \in M$ and scalars $a_{i,j} \in R$ (where $i \in 1 \dots m$ and $j \in J$) such that only finitely many $a_{i,j}$ are non-zero [that is $\#\{ (i,j) \in 1 \dots m \times J \mid a_{i,j} \neq 0 \} < \infty$] such that the following two properties hold true

$$\begin{aligned}
\forall\, i \in 1 \dots m &: \sum_{j \in J} a_{i,j} n_j = 0 \\
\forall\, j \in J &: m_j = \sum_{i=1}^{m} a_{i,j} x_j
\end{aligned}$$

(3.154) Proposition: (viz. 1134)
Let $(E, +, \cdot)$ be a field and $M_1, \dots, M_n$ be E-modules (which are free automatically, since E is a field). Now consider some elements $x_i, y_i \in M_i$ (where $i \in 1 \dots n$), then we obtain the following statements

(i) The tensor product $x_1 \otimes \dots \otimes x_n = 0$ is zero if and only if we have $x_i = 0$ for some $i \in 1 \dots n$ [the implication $\exists\, i \in 1 \dots n : x_i = 0 \implies x_1 \otimes \dots \otimes x_n = 0$ is true over arbitrary commutative rings, the converse direction uses the fact that all the M_i are free, however].

(ii) We have the equality $x_1 \otimes \ldots \otimes x_n = y_1 \otimes \ldots \otimes y_n \neq 0$ if and only if there are some $a_1, \ldots, a_n \in E$ such that (1) $y_i = a_i x_i$ for all $i \in 1 \ldots n$ and (2) $a_1 \ldots a_n = 1$.

(iii) For any $i \in 1 \ldots n$ let $X_i \subseteq M_i$ be a non-empty ($X_i \neq \emptyset$) subset of M_i and let us denote the following subset of $M_1 \otimes \ldots \otimes M_n$

$$X_1 \otimes \ldots \otimes X_n \;:=\; \{\, x_1 \otimes \ldots \otimes x_n \mid \forall\, i \in 1 \ldots n : x_i \in X_i \,\}$$

Now let $\star$ replace any of the properties *generates*, *is a linear independent subset of* or *is a basis of*. Then we get the following three implications

$$\forall\, i \in 1 \ldots n \;:\; X_i \;\star\; M_i \quad\Longrightarrow\quad X_1 \otimes \ldots \otimes X_n \;\star\; M_1 \otimes \ldots \otimes M_n$$

[Note that the assumption of E being a field is only required for $\star =$ *is linear independent in*. The other two implications remain true over arbitrary commutative rings E].

(iv) If $U_i \;\leq_{\mathsf{m}}\; M_i$ (where $i \in 1 \ldots n$) are subspaces of the M_i then the map $\otimes_{i=1}^n U_i \to \otimes_{i=1}^n M_i : \otimes_{i=1}^n x_i \mapsto \otimes_{i=1}^n x_i$ is injective. And in this sense we can interpret $\otimes_{i=1}^n U_i \;\leq_{\mathsf{m}}\; \otimes_{i=1}^n M_i$ as a subspace of $M_1 \otimes \ldots \otimes M_n$ again

$$\bigotimes_{i=1}^n U_i = \left\{ \sum_{k=1}^m a_k\, u_{1,k} \otimes \ldots \otimes u_{n,k} \;\middle|\; a_k \in E, u_{i,k} \in M_i \right\} \leq_{\mathsf{m}} \bigotimes_{i=1}^n M_i$$

And if $U_{i,j} \;\leq_{\mathsf{m}}\; M_i$ (where $j \in J(i)$) are arbitrary families of subspaces of the M_i, then we also find the following equality of subsets of $M_1 \otimes \ldots \otimes M_n$

$$\bigotimes_{i=1}^n \left(\bigcap_{j \in J(i)} U_{i,j} \right) \;=\; \bigcap_{j \in J(1) \times \ldots J(n)} \bigotimes_{i=1}^n U_{i,j(i)}$$

(v) Let again $U_i \;\leq_{\mathsf{m}}\; M_i$ (where $i \in 1 \ldots n$) be subspaces of the M_i and consider some $a_k \in E$ with $a_k \neq 0$ and $x_{i,k} \in M_i$ (where $i \in 1 \ldots n$ and $k \in 1 \ldots m$) such that for any $i \in 1 \ldots n$ the set $\{\, x_{i,k} \mid k \in 1 \ldots m \,\} \subseteq M_i$ is linear independent. Then we get the equivalence

$$\sum_{k=1}^m a_k\, x_{1,k} \otimes \ldots \otimes y_{i,k} \;\in\; \bigotimes_{i=1}^n U_i \quad\Longleftrightarrow\quad \begin{array}{c} \forall\, i \in 1 \ldots n \\ \forall\, k \in 1 \ldots m \\ x_{i,k} \in U_i \end{array}$$

We will now restrict to the case $n = 2$, that is we consider any two modules M and N over the field E. Then we further get the following statements:

(vi) If $x_1, \ldots, x_m \in M$ are linear independent and $y_1, \ldots, y_m \in N$ and $y'_1, \ldots, y'_m \in N$ are arbitrary elements in N, then we get

$$\sum_{k=1}^m x_k \otimes y_k \;=\; \sum_{k=1}^m x_k \otimes y'_k \quad\Longrightarrow\quad \forall\, k \in 1 \ldots m \;:\; y_k = y'_k$$

(vii) Now pick up an arbitrary tensor element $t = \sum_{k=1}^{m} a_k\, x_k \otimes y_k \in M \otimes N$. Then the number m of pure tensors in this representation is minimal (that is $m = \mu(t)$) iff all of the following three conditions are met

(1) $\forall\, k \in 1 \ldots m \;:\; a_k \neq 0$

(2) $\{\, x_k \mid k \in 1 \ldots m \,\} \subseteq M$ is E-linearly independent

(3) $\{\, y_k \mid k \in 1 \ldots m \,\} \subseteq N$ is E-linearly independent

In particular every tensor element $t \in M \otimes N$ admits a representation $t = \sum_r a_r\, u_r \otimes v_r$ with $a_r \neq 0$ and $\{\, u_1, \ldots, u_s \,\} \subseteq M$ and $\{\, v_1, \ldots, v_s \,\} \subseteq N$ E-linearly independent.

(3.155) Theorem: (viz. 1145)
Let $(R, +, \cdot)$ be a commutative ring and M and N be R-modules. Then we obtain the following statements

(i) If M is finitely generated and $\star$ abbreviates any one of the following properties *finitely generated*, *noetherian* or *artinian*, then we get the following implication:

$$N \text{ is } \star \quad \Longrightarrow \quad M \otimes N \text{ is } \star$$

(ii) And if $\star$ abbreviates any one of the properties *finitely generated*, *free*, *noetherian*, *artinian* or *has a finite free presentation*, then we get the following implication:

$$M \text{ and } N \text{ are } \star \quad \Longrightarrow \quad M \otimes N \text{ is } \star$$

(iii) Moreover, if both M and N have finite length, then the tensor product has finite length, as well and we find the inequality

$$\ell(M \otimes N) \;\leq\; \ell(M) \cdot \ell(N)$$

(iv) In the fancy language of homological algebra the following property can be put shortly as: *The tensor functor is right-exact*. This is to say: Consider any exact chain of R-modules, of the form

$$U \xrightarrow{\varphi} V \xrightarrow{\psi} W \to 0$$

Then tensoring such a chain with M from the right, we obtain another exact chain of R-modules

$$U \otimes M \xrightarrow{\varphi \otimes M} V \otimes M \xrightarrow{\psi \otimes M} W \otimes M \to 0$$

(v) Consider two *right-exact* chains of R-modules, i.e. exact chains of R-modules, of the following form

$$M_0 \xrightarrow{\varphi_1} M_1 \xrightarrow{\varphi_2} M_2 \to 0$$

$$N_0 \xrightarrow{\psi_1} N_1 \xrightarrow{\psi_2} N_2 \to 0$$

Then we can explicitly give the kernel of the tensor map $\varphi_2 \otimes \psi_2$ to be the following submodule

$$\mathrm{kn}(\varphi_2 \otimes \psi_2) \;=\; \mathrm{im}(\varphi_1 \otimes N_1) + \mathrm{im}(M_1 \otimes \psi_1)$$

(3.156) Remark:
As we have just seen in, the tensor product preserves right-exact chains of R-modules. This already implies, that the tensor product preserves surjectivity. This is to say: Consider any R-modules M, U and V over a commutative ring $(R, +, \cdot)$ and let $\varphi : U \twoheadrightarrow V$ be a surjective homomorphism of R-modules. Then the map $\varphi \otimes M$ is surjective, as well:

$$\varphi \otimes M \ : \ U \otimes M \ \twoheadrightarrow \ V \otimes M$$

Prob we can extend $\varphi : U \twoheadrightarrow V$ to an exact chain $\ker(\varphi) \to U \to V \to 0$, by taking $\subseteq : \ker(\varphi) \to U$ as a homomorphism. Then by (3.155.(vi)) $\ker(\varphi) \otimes M \to U \otimes M \to V \otimes M \to 0$ is exact again. In particular $\varphi \otimes M : U \otimes M \to V \otimes M$ is surjective.

(3.157) Example:
Note that the right-exactness of the tensor functor cannot be generalized, as a counter-example consider the following exact chain of $\mathbb{Z}$-modules

$$0 \to \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z}$$

where $\cdot 2$ denotes the linear map $k \mapsto 2k$. Tensoring this with $\mathbb{Z}_2$ we arrive the following non-exact chain of modules (see below). It is non-exact, as for any $k \in \mathbb{Z}$ and any $b \in \mathbb{Z}_2$ we clearly have $k \otimes b \mapsto (2k) \otimes b = k \otimes (2b) = k \otimes 0 = 0$, hence $\cdot 2 \otimes \mathbb{1}$ is the zero-homomorphism and thereby certainly not injective, as $\mathbb{Z} \otimes \mathbb{Z}_2 \ \cong_{\mathfrak{m}} \ \mathbb{Z}_2$.

$$0 \to \mathbb{Z} \otimes \mathbb{Z}_2 \xrightarrow{\cdot 2 \otimes \mathrm{id}} \mathbb{Z} \otimes \mathbb{Z}_2$$

Change of Base Rings:

(3.158) Definition:
Suppose $(R, +, \cdot)$ is a commutative ring, M is an R-module and S is an R-algebra. Then $S \otimes M$ is an R-module, but in complete analogy to (3.144.(iii)) above it also is an S-module under the scalar multiplication (where $a_i \in R$, $x_i \in M$ and $r, s_i \in S$)

$$r \left(\sum_{i=1}^{n} a_i \, s_i \otimes x_i \right) \ := \ \sum_{i=i}^{n} a_i \, (r s_i) \otimes x_i$$

That is by tensoring the R-module M with S we end up with an S-module $S \otimes M$. This construction is hence known as *change of base rings*. And we will denote

$$M_S \ := \ S \otimes M$$

to emphasize that we now regard M_S as an S-module (not as an R-module any longer). Recall that given two R-modules M and N and an R-module homomorphism $\varphi : M \to N$ we also get an R-module homomorphism $S \otimes \varphi$ by virtue of

$$\varphi_S \ := \ S \otimes \varphi \ : \ \sum_{i=1}^{n} a_i \, s_i \otimes x_i \mapsto \sum_{i=1}^{n} a_i \, s_i \otimes \varphi(x_i)$$

If r, $s \in S$ and $x \in M$, then $\varphi_S(r(s \otimes x)) = \varphi_S((rs) \otimes x) = (rs) \otimes \varphi(x) = r(s \otimes \varphi(x)) = r\varphi_S(s \otimes x)$ such that φ_S already is S-linear, too. Therefore we can always regard φ_S as an S-module-homomorphism from M_S to N_S.

(3.159) Example: (viz. 1143)
Let us recollect some examples of (3.146) that illustrate why the name "change of base rings" is well-chosen: If $(R, +, \cdot)$ is a commutative ring, M is an R-module, $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ is an ideal and $U \subseteq R$ is a multiplicatively closed set, then we have the following isomorphies [of modules over the new base ring, that is as R-, $(R/\mathfrak{a})$- or resp. of $U^{-1}R$-modules]

$$M_R \xrightarrow{\sim} M : a \otimes x \mapsto ax$$

$$M_{R/\mathfrak{a}} \xrightarrow{\sim} M \Big/ {}_{\mathfrak{a}M} : (b + \mathfrak{a}) \otimes x \mapsto bx + \mathfrak{a}M$$

$$M_{U^{-1}R} \xrightarrow{\sim} U^{-1}M : \frac{a}{u} \otimes x \mapsto \frac{ax}{u}$$

And if S is an arbitrary R-algebra, $(A, +)$ is a commutative monoid, then the change of base rings turns the R-algebra of polynomials over R into the S-algebra of polynomials over S. That is we find an isomorphy of S-algebras, by linear expansion of

$$R[t \mid A]_S \xrightarrow{\sim} S[t \mid A] : s \otimes f \mapsto sf$$

Also if the R-algebra S satisfies $\{ a1_S \mid a \in R \} \subseteq \mathrm{CEN}(S)$ and we fix some $1 \leq m$, $n \in \mathbb{N}$ then the change of base rings turns the R-algebra of matrices over R into the S-algebra of matrices over S. That is we find an isomorphy of S-algebras, by linear expansion of

$$\Big(\mathrm{mat}_{m,n}(R)\Big)_S \xrightarrow{\sim} \mathrm{mat}_{m,n}(S) : s \otimes A \mapsto sA$$

Note that in all of these examples the pure tensor $s \otimes x$ is mapped onto the scalar product sx of the "traditional" S-module. This illustrates how canonical the change of base rings is.

(3.160) Proposition: (viz. 1139)
Let $(R, +, \cdot)$ be a commutative ring, S be an (not necessarily commutative) R-algebra and let M be an R-module. Then we get the following properties

(i) If M is a free R-module, with R-basis $\{ m_i \mid i \in I \}$ then M_S is a free S-module with S-basis $\{ 1_S \otimes m_i \mid i \in I \}$. In particular we get

$$\dim_S(M_S) = \dim_R(M)$$

(ii) $(\diamondsuit)$ Let M be a free R-module with finite basis $\{ m_j \mid j \in 1 \ldots n \}$ again. Also let N be a free R-module with finite basis $\{ n_i \mid i \in 1 \ldots m \}$. Finally let $\varphi : M \to N$ be an R-module-homomorphism with matrix representation $[\varphi] = (a_{i,j}) \in \mathrm{mat}_{m,n}(R)$, that is

$$\varphi(m_j) = \sum_{i=1}^{m} a_{i,j} n_i$$

If we now fix the S-bases $\{ 1_S \otimes m_j \mid j \in 1 \ldots n \}$ on M_S and likewise $\{ 1_S \otimes n_i \mid i \in 1 \ldots m \}$ on N_S, then $\varphi_S : M_S \to N_S$ has the basis representation $[\varphi] = (a_{i,j} 1_S) \in \mathrm{mat}_{m,n}(S)$, that is

$$\varphi(1_S \otimes m_j) \;=\; \sum_{i=1}^{m} (a_{i,j} 1_S)(1_S \otimes n_i)$$

(iii) If $S \neq 0$ is a free R-algebra, then the canonical homomorphism $M \hookrightarrow M_S : x \mapsto 1_S \otimes x$ is injective.

(iv) *Transitivity of the Change of base Rings*: If A is a commutative R-algebra and B is a (not necessarily commutative) A-algebra, then we find the following isomorphy of B-modules:

$$\Big(M_A\Big)_B \xrightarrow{\sim} M_B \;:\; b \otimes (a \otimes x) \mapsto (ab) \otimes x$$

(v) If S is a commutative R-algebra and $M(i)$ is a family of R-modules (where $i \in 1 \ldots n$) then the change of base rings is compatible with the tensor product: We obtain an isomorphy of S-modules

$$\big(M(1) \otimes_R \ldots \otimes_R M(n)\big)_S \quad\xrightarrow{\sim}\quad M(1)_S \otimes_S \ldots \otimes_S M(n)_S$$

$$1_S \otimes (x_1 \otimes \ldots \otimes x_n) \quad\mapsto\quad (1_S \otimes x_1) \otimes \ldots \otimes (1_S \otimes x_n)$$

(vi) Consider an S-module N, this can be turned into an R-module, as well, using the scalar multiplication $an := (a1_S)n$. If now $\varphi : M \to N$ is an R-module-homomorphism [that is $\varphi(ax) = (a1_S)\varphi(x)$] then there is a uniquely determined S-module-homomorphism $\varphi_{(S)} : M_S \to N$ such that for any $x \in M$ we get $\varphi_{(S)}(1_S \otimes m) = \varphi(x)$. And this is given by

$$\varphi_{(S)} \;:\; M_S \to N \;:\; \sum_{k=1}^{m} a_k s_k \otimes x_k \mapsto \sum_{k=1}^{m} (a_k s_k)\varphi(x_k)$$

And we thereby find that the map $\varphi \mapsto \varphi_S$ is an isomorphism of R-modules whose inverse is given to be $\psi \mapsto (x \mapsto \psi(1_S \otimes x))$, altogether that is

$$\begin{array}{rcl} \mathrm{mhom}_R(M,N) & \xrightarrow{\sim} & \mathrm{mhom}_S(M_S,N) \\ \varphi & \mapsto & \varphi_{(S)} \\ \big(x \mapsto \psi(1_S \otimes x)\big) & \leftarrow\!\shortmid & \psi \end{array}$$

If S is commutative then this map even is an isomorphism of S-modules [note that since N is an S-module $s\varphi : x \mapsto s\varphi(x)$ makes sense].

(vii) If A is an R-(semi-)algebra, B is an S-(semi-)algebra and $\varphi : A \to B$ is a homomorphism of R-(semi-)algebras, then $\varphi_{(S)} : A_S \to B$ is a homomorphism of S-(semi-)algebras again.

(3.161) Proposition: (viz. 1142)
Let $(E,+,\cdot)$ be a field, S a (not necessarily commutative) E-algebra and consider two E-vector-spaces U and V. If now $\varphi : U \to V$ is any E-linear map, then we get the following properites:

(i) Let $\star$ abbreviate any of the words *injective*, *surjective* or *bijective* and suppose φ is $\star$. Then the induced map φ_S is $\star$ as well

$$\varphi \text{ is } \star \iff \varphi_S \text{ is } \star$$

(ii) If $\{ u_i \mid i \in I \} \subseteq U$ is an E-basis of $\mathrm{kn}(\varphi)$, then $\{ 1_S \otimes u_i \mid i \in I \} \subseteq U_S$ is a S-basis of $\mathrm{kn}(\varphi_S)$. And thereby we can write the kernel of φ_S in the following form

$$\mathrm{kn}(\varphi_S) \;=\; \mathrm{Lh}_S\{ 1_S \otimes u \mid u \in \mathrm{kn}(\varphi) \}$$

(iii) If $\{ v_j \mid j \in J \} \subseteq V$ is an E-basis of $\mathrm{im}(\varphi)$, then $\{ 1_S \otimes v_j \mid j \in J \} \subseteq V_S$ is a S-basis of $\mathrm{im}(\varphi_S)$. And thereby we can write the image of φ_S in the following form

$$\mathrm{im}(\varphi_S) \;=\; \mathrm{Lh}_S\{ 1_S \otimes v \mid v \in \mathrm{im}(\varphi) \}$$

(iv) If S is a field as well, then φ and φ_S share the same rank (over their respective base fields), i.e.

$$\mathrm{rank}_S(\varphi_S) \;=\; \mathrm{rank}_E(\varphi)$$

(3.162) Proposition: (viz. 1143)
As always let $(R,+,\cdot)$ be a commutative ring and consider M, N two R-modules. Also let $S \neq 0$ be an arbitrary non-zero R-algebra. Then we obtain a well-defined, S-linear map, by S-linear expansion of

$$\mu \;:\; \big(\mathrm{mhom}_R(M,N)\big)_S \to \mathrm{mhom}_S(M_S,N_S)$$

$$\mu \;:\; s \otimes \varphi \mapsto s\,\varphi_S$$

(i) If S is free, then μ is injective.

(ii) If S is free and finite-dimensional, then μ is bijective.

(iii) If M and N are free and finite-dimensional, then μ is bijective.

(3.163) Example:
The most common application of the change of base rings is the *complexification of real vector spaces*, that is we start with an $\mathbb{R}$-vectorspace V and use change of base rings to replace $\mathbb{R}$ by $\mathbb{C}$

$$V_{\mathbb{C}} \;=\; \mathbb{C} \otimes_{\mathbb{R}} V$$

As $\mathbb{C}$ is a free $\mathbb{R}$-algebra, having the basis $\{1,i\}$, we can interpret V as a subspace of $V_{\mathbb{C}}$ under the canonical embedding

$$V \hookrightarrow V_{\mathbb{C}} \;:\; x \mapsto 1 \otimes x$$

And if $\{ v_k \mid k \in K \} \subseteq V$ is an $\mathbb{R}$-basis of V, then $V_{\mathbb{C}}$ has the $\mathbb{C}$-basis $\{ 1 \otimes v_k \mid k \in K \}$ again. On the other hand (3.146.(vi)) tells us, that an $\mathbb{R}$-basis of $V_{\mathbb{C}}$ is now given, by $\{ 1 \otimes v_k \mid k \in K \} \cup \{ i \otimes v_k \mid k \in K \}$. Using the embedding $x \mapsto 1 \otimes x$ we find that $1 \otimes v_k = v_k$ and $i \otimes v_k = i(1 \otimes v_k) = iv_k$. That is $V_{\mathbb{C}}$ has the $\mathbb{R}$-basis $\{ v_k \mid k \in K \} \cup \{ iv_k \mid k \in K \}$ and therefore

$$\dim_{\mathbb{C}}(V_{\mathbb{C}}) \;=\; \dim_{\mathbb{R}}(V) \text{ and } \dim_{\mathbb{R}}(V_{\mathbb{C}}) \;=\; 2 \cdot \dim_{\mathbb{R}}(V)$$

Hence the complexification $V_{\mathbb{C}}$ is isomorphic (as an $\mathbb{R}$-vectorspace) to two copies $V \oplus V$ of V under the following $\mathbb{R}$-vectorspace isomorphism. And under this isomorphism the scalar multiplication $\mathbb{C} \times V_{\mathbb{C}} \to V_{\mathbb{C}}$ which is given by $(c, x) \mapsto c \otimes x$ becomes the following $\mathbb{R}$-bilinear map

$$V \oplus V \;\xrightarrow{\sim}\; V_{\mathbb{C}} \;:\; \left(\sum_{k \in K} a_k v_k, \sum_{k \in K} b_k v_k \right) \mapsto \sum_{k \in K} (a_k + ib_k) \otimes v_k$$

$$\mathbb{C} \times V^{\oplus 2} \to V^{\oplus 2} \;:\; (a + bi, (x, y)) \mapsto (ax - by, bx + ay)$$

Many ad-hoc constructions of $V_{\mathbb{C}}$ employ this technique: They define $\mathbb{V}_{\mathbb{C}}$ to be $V^{\oplus 2}$ and define the scalar multiplication $\mathbb{C} \times V^{\oplus 2} \to V^{\oplus 2}$ using this $\mathbb{R}$-bilinear map. While there's nothing wrong with that, it remains to prove the properties of a $\mathbb{C}$-vectorspace, in this case.

3.14 Direct Limits

This section is somewhat more advanced and can be safely skipped, at a first reading. We will introduce two constructions, the direct and inverse limits of modules. These will be the algebraic answer to problems of approximation and convergence. A special case are adic completions and completion of topological spaces. You already see here, that this concept is quite general - it can be done with groups, rings, modules, ... even with topological spaces. This is where we will use or $\star$ again. We will not take the categorial point of view yet, but regard several categories at once - without the formal background. E.g. we are primarily interested in modules M over a fixed, commutative ring $(R, +, \cdot)$. Then the *objects* are R-modules and the *morphisms* are R-module-homomorphisms - that is R-linear maps. We will regard related situations simultaneously. Hence throughout this section we install the following nomenclature: We speak of $\star$-objects and the corresponding $\star$-morphisms, as summarized in the following table.

$\star$-objects	$\star$-morphisms	$\hom(M,N)$
sets	functions	$\mathcal{F}(M,N)$
(commutative) groups	group-homomorphisms	$\mathrm{ghom}(M,N)$
R-modules	R-module-homomorphisms	$\mathrm{mhom}(M,N)$
(commutative) rings	ring-homomorphisms	$\mathrm{rhom}(M,N)$
(commutative) R-algebras	R-algebra-homomorphisms	$\mathrm{ahom}(M,N)$
topological spaces	continuous maps	$C(M,N)$

Note that in case of R-modules and R-algebras, the base ring R is assumed to be commutative and the same for all $\star$-objects. The notion of topological spaces will be introduced in section 6.1. As they play a special role, let us agree to call the upper five kinds of $\star$-objects (that is all here, except topological spaces) *algebraic*. So if we say that M is an algebraic $\star$-object, we mean a set, R-module or (commutative) group, ring resp. R-algebra - but not a topological space. Let us now begin with the first half: **inverse limits**. This are sometimes also called **projective limits** of simply **limits**.

(3.164) Definition:
Let $(I, \leq)$ be a fixed partially ordered set. We say that (M_i, μ_j^i) is an **inverse system** of $\star$-objects over I, iff the following four properties are satisfied

(1) $\forall\, i \in I$ we get: M_i is a $\star$-object

(2) $\forall\, i, j \in I$ with $i \leq j$ we get: $\mu_j^i : M_j \to M_i$ is a $\star$-morphism

(3) $\forall\, i \in I$ we get: $\mu_i^i : M_i \to M_i : x \mapsto x$ is the identity map on M_i

(4) $\forall\, i, j$ and $k \in I$ with $i \leq j$ and $j \leq k$ we get: $\mu_j^i \mu_k^j = \mu_k^i$

And in this case we define the **inverse limit** of the inverse system (M_i, μ_j^i) to be the set of all sequences (x_i) that always satisfy $x_i = \mu_j(x_i)$ for all $i \leq j \in I$. Formally, that is

$$\varprojlim (M_i,\, \mu_j^i) \;:=\; \left\{ (x_i) \in \prod_{i \in I} M_i \;\middle|\; \forall\, i \leq j \in I \,:\, x_i = \mu_j^i(x_i) \right\}$$

Clearly the inverse limit allows to define the **canonical projections** π_j for any $j \in I$, that map (x_i) to x_j. And from the construction of the inverse limit it is clear, that for any $i \leq j \in I$ we get $\mu_j^i \pi_j = \pi_i$, where

$$\pi_j \;:\; \varprojlim (M_i,\, \mu_j^i) \;\to\; M_j \;:\; (x_i) \;\mapsto\; x_j$$

Recall, that a **net** (which some authors refer to, as a **filtered set**) is a non-empty, partially ordered set $(I, \leq)$, such that for any two elements $i, j \in I$ there is an $k \in I$, such that $k \geq i$ and $k \geq j$. By induction it is clear, that thereby for any finite subset $\{\, i_1, \ldots, i_n \,\} \subseteq I$ there is some $k \in I$ such that $k \geq i_r$ for any $r \in 1 \ldots n$. At times we will require this additional property in this section, as in (v) below:

(3.165) Proposition: (viz. 772)

(i) If (G_i, γ_j^i) is an inverse system of (commutative) groups, over the partially ordered set $(I, \leq)$, then its inverse limit is a (commutative) group again, under the pointwise composition $(x_i)(y_i) := (x_i y_i)$. And its neutral element is given to be (e_i) where $e_i \in G_i$ are the respective neutral elements.

(ii) Fix a commutative ring $(R, +, \cdot)$. If (M_i, μ_j^i) is an inverse system of R-modules, over the partially ordered set $(I, \leq)$, then its inverse limit is an R-module again, under the pointwise addition $(x_i) + (y_i) := (x_i + y_i)$ and scalar multiplication $a(x_i) := (a x_i)$.

(iii) If (R_i, ϱ_j^i) is an inverse system of (commutative) rings, over the partially ordered set $(I, \leq)$, then its inverse limit is a (commutative) ring again, under the pointwise addition $(a_i) + (b_i) := (a_i + b_i)$ and multiplication $(a_i) \cdot (b_i) := (a_i \cdot b_i)$. And its unit element is given to be (1_i) where $1_i \in R_i$ are the respective unit elements.

(iv) Fix a commutative ring $(R, +, \cdot)$. If (A_i, α_j^i) is an inverse system of R-algebras, over the partially ordered set $(I, \leq)$, then its inverse limit is an R-algebra again, under the pointwise addition $(f_i) + (g_i) := (f_i + g_i)$, multiplication $(f_i) \cdot (g_i) := (f_i \cdot g_i)$ and scalar-multiplication $a(f_i) := (a f_i)$. And its unit element is given to be (1_i) where $1_i \in A_i$ are the respective unit elements.

(v) If (X_i, f_j^i) is an inverse system of topological spaces $(X_i, \mathcal{T}_i)$, over the net $(I, \leq)$, then its inverse limit becomes a topological space again: Let $X_\infty := \varprojlim (X_i, f_j^i)$ abbreviate the inverse limit. The topology on X_∞ is taken to be the coarsest topology, such that all the canonical projections $\pi_j : X_\infty \to X_j : (x_i) \mapsto x_i$ are continuous. This is called the **limit topology** of X_∞ and a base of this topology is given by

$$\mathcal{W} \;:=\; \left\{\, \pi_i^{-1}(U_i) \;\middle|\; i \in I,\; U_i \subseteq X_i \text{ open} \,\right\}$$

In this particular case we get a concrete description of this topology in the following terms: A set $C \subseteq X_\infty$ is closed if and only if there is a sequence of closed subsets $C_i \subseteq X_i$, such that

$$C \;=\; \bigcap_{i \in I} \pi_i^{-1}(C_i)$$

(3.166) Example:

(i) Fix any commutative ring $(R,+,\cdot)$ and the index set $I := \mathbb{N}$. For any $n \in \mathbb{N}$ we regard the ring $R_n := R[t]/t^nR[t]$. That is $R_0 = 0$, $R_1 = R$ and so on. For any $m \leq n \in \mathbb{N}$ we define the transition map (which is well defined, as $t^nR[t] \subseteq t^mR[t]$)

$$\tau_n^m \;:\; R_n \;\twoheadrightarrow\; R_m \;:\; f + t^nR[t] \;\mapsto\; f + t^mR[t]$$

Then the inverse limit of this inverse system is isomorphic to the ring of formal power series over R. That is the following map is an isomorphism of rings

$$\begin{array}{rcl} R[\![t]\!] & \xrightarrow{\sim} & \varprojlim (R_n, \tau_n^m) \\ \displaystyle\sum_{k=0}^{\infty} a_k t^k & \mapsto & \left(\displaystyle\sum_{k=0}^{n-1} a_k t^k + t^nR[t] \right) \end{array}$$

(ii) The example in (i) above is a special case of the following more general situation: Fix a commutative ring $(R,+,\cdot)$ and an ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$. Over the index set $I := \mathbb{N}$ again, let $R_n := R/\mathfrak{a}^n$. As for $m \leq n$ we have $\mathfrak{a}^n \subseteq \mathfrak{a}^n$ the following transition maps are well defined, again

$$\tau_n^m \;:\; R_n \;\twoheadrightarrow\; R_m \;:\; b + \mathfrak{a}^n \;\mapsto\; n + \mathfrak{a}^m$$

This becomes (i) by taking $R[t]$ for R and $tR[t]$ for $\mathfrak{a}$. The inverse limit of this inverse system of commutative rings is said to be the **$\mathfrak{a}$-adic completion** of R. It is usually denoted by

$$\widehat{R} \;:=\; \varprojlim (R_n, \tau_n^m)$$

If the intersection $\bigcap_n \mathfrak{a}^n = 0$ vanishes, where $n \in \mathbb{N}$, then it is immediate to see, that we find a monomorphism of rings from R into its completion, simply by taking

$$R \;\hookrightarrow\; \widehat{R} \;:\; b \;\mapsto\; (b + \mathfrak{a}^n)$$

(iii) The following example is a little minimalistic and artificial, but instructive: Consider any two commutative rings $(R,+,\cdot)$ and $(S,+,\cdot)$ and a homomorphism of rings $\varphi : R \to S$ between them. We get an inverse system of commutative rings over $I := \{1,2\}$ by taking $R_2 := R$, $R_1 := S$ and $\varphi_2^1 := \varphi$. Let L denote the inverse limit of this indirect system, then the elements of L are pairs $(a,b) \in R \times S$ where $b = \varphi(s)$. That is

$$L \;=\; \{\, (a, \varphi(a)) \mid a \in R \,\} \;\subseteq\; R \oplus S$$

Thus we see, that the canonical projection $\pi_2 : L \to S$ maps $\pi_2(a,\varphi(a)) = \varphi(a)$ and hence need not be surjective in general. It will be surjective, if φ is such, but even this will not be true, for general inverse limits.

(iv) If the index set I has a maximal element $m \in I$, that is $i \leq m$ for any $i \in I$, then the inverse limit will be isomorphic to M_m. Hereby π_m is a $\star$-morphism and its inverse morphism is given to be

$$M_m \xrightarrow{\sim} \varprojlim (M_i, \mu_j^i) \ : \ x \mapsto (\mu_m^i(x))$$

We now turn our attention to the dual notion: **direct limits**, which some authors also call **colimits**. While inverse limits have been in the opposite direction of the index set, direct limits will be in the direction of the index set. The constructions will only be little more complicated, but the properties will be surprisingly different. Inverse limits usually are better behaved, than direct limits.

(3.167) Definition: (viz. 773)
Let $(I, \leq)$ be a fixed net. We say that (M_i, μ_j^i) is a **direct system** of $\star$-objects over I, iff the following four properties are satisfied

(1) $\forall\, i \in I$ we get: M_i is a $\star$-object

(2) $\forall\, i, j \in I$ with $i \leq j$ we get: $\mu_i^j : M_i \to M_j$ is a $\star$-morphism

(3) $\forall\, i \in I$ we get: $\mu_i^i : M_i \to M_i : x \mapsto x$ is the identity map on M_i

(4) $\forall\, i, j$ and $k \in I$ with $i \leq j$ and $j \leq k$ we get: $\mu_j^k \mu_i^j = \mu_i^k$

And in this case we define the **direct limit** of the direct system (M_i, μ_i^j) to be the disjoint union of the M_i under a certain equivalence relation $\sim$. Formally we define:

$$\varinjlim (M_i, \mu_i^j) := \mathcal{M} \Big/ \sim \quad \text{where} \quad \mathcal{M} := \bigcup_{i \in i} \{\, i \,\} \times M_i$$
$$\text{and} \quad (i, x) \sim (j, y) \ :\Longleftrightarrow \ \exists\, k \geq i, j \ : \ \mu_i^k(x) = \mu_j^k(y)$$

Nota this definition encompasses $(i, x) \sim (j, \mu_i^j(x))$ for any $j \geq i$. And clearly the direct limit allows to define the **structure morphisms** ε_i for any $i \in I$, that map x_i to its equivalence class $[i, x_i]$. And from the construction of the direct limit it is clear, that for any $i \leq j \in I$ we get $\varepsilon_j \mu_i^j = \varepsilon_i$, where

$$\pi_i \ : \ M_i \to \varinjlim (M_i, \mu_i^j) \ : \ x_i \mapsto [i, x_i]$$

(3.168) Proposition: (viz. 773)

(i) If (G_i, γ_i^j) is an direct system of (commutative) groups, over the net $(I, \leq)$, then its direct limit is a (commutative) group again, under the following composition: Given $[i, x]$ and $[j, y]$ choose any $k \in I$ with $k \geq i, j$, then $[i, x][j, y] := [k, \gamma_i^k(x)\gamma_j^k(y)]$. And its neutral element is given to be $[i, e_i]$ where $e_i \in G_i$ is the respective neutral element and $i \in I$ is arbitrary.

(ii) Fix a commutative ring $(R, +, \cdot)$. If (M_i, μ_j^i) is an direct system of R-modules, over the net $(I, \leq)$, then its direct limit is an R-module again, under the following addition and scalar multiplication: Given $[i, x]$ and $[j, y]$ choose any $k \in I$ with $k \geq i, j$, then $[i, x] + [j, y] := [k, \mu_i^k(x) + \mu_j^k(x)]$. And given $a \in R$ define $a[i, x] := [i, ax]$.

(iii) If (R_i, ϱ_j^i) is an inverse system of (commutative) rings, over the net $(I, \leq)$, then its direct limit is a (commutative) ring again, under the following addition and multiplication: Given $[i,a]$ and $[j,a]$ choose any $k \in I$ with $k \geq i, j$, then $[i,a] + [j,b] := [k, \varrho_i^k(a) + \varrho_j^k(b)]$ and likewise $[i,a] \cdot [j,b] := [k, \varrho_i^k(a) \cdot \varrho_j^k(b)]$. And its unit element is given to be $[i,1_i]$ where $1_i \in R_i$ is the respective unit element and $i \in I$ is arbitrary.

(iv) Fix a commutative ring $(R,+,\cdot)$. If (A_i, α_j^i) is a direct system of R-algebras, over the net $(I,\leq)$, then its direct limit is an R-algebra again, under the following addition and multiplication: Given $[i,f]$ and $[j,g]$ choose any $k \in I$ with $k \geq i, j$, then $[i,f] + [j,g] := [k, \alpha_i^k(f) + \alpha_j^k(g)]$ and likewise $[i,f] \cdot [j,g] := [k, \alpha_i^k(f) \cdot \alpha_j^k(g)]$. And its unit element is given to be $[i,1_i]$ where $1_i \in R_i$ is the respective unit element and $i \in I$ is arbitrary.

(v) If (X_i, f_i^j) is a direct system of topological spaces $(X_i, \mathcal{T}_i)$, over the net $(I,\leq)$, then its direct limit becomes a topological space again: Let $X_\infty := \varprojlim (X_i, f_j^i)$ abbreviate the direct limit. The topology on X_∞ is taken to be the coarsest topology, such that all the structure morphisms are continuous $\varepsilon_i : X_i \to X_\infty : x_i \mapsto [i,x_i]$. This is called the **limit topology** of X_∞ again and (by definition) a subset $U \subseteq X_\infty$ is open, if and only if

$$U \subseteq X_\infty \text{ open} \quad :\Longleftrightarrow \quad \forall\, i \in I : \varepsilon_i^{-1}(U) \subseteq X_i \text{ open}$$

(3.169) Proposition: (viz. 775)
Let (M_i, μ_i^j) be a direct system of $\star$-objects over the net $(I,\leq)$ and abbreviate its direct limit by M_∞. Then for any $i \in I$ the structure morphism $\varepsilon_i : M_i \to M_\infty$ is a $\star$-morphism. And if all of the transition maps μ_i^j are injective, then so are the ε_i.
In the case of topological spaces we also get the following statement: If all of the transition maps μ_i^j are open maps, then so are the structure morphisms ε_i.

(3.170) Example: (viz. 776)

(i) Let us consider our minimalistic example in the context of direct limits: Consider any two commutative rings $(R,+,\cdot)$ and $(S,+,\cdot)$ and a homomorphism of rings $\varphi : R \to S$ between them. We get a direct system of commutative rings over $I := \{1,2\}$ by taking $R_1 := R$, $R_2 := S$ and $\varphi_1^2 := \varphi$. Let L denote the direct limit of this indirect system, then the elements of L are either $[1,a]$ for some $a \in R$ or $[2,f]$ for some $f \in S$. Thereby $[1,a] = [2,f]$ iff $f = \varphi(a)$. Thus all the elements of R are absorbed in L in the form $[2,\varphi(a)]$. Hence it is not much of a surprise, that

$$\varepsilon_2 \,:\, S \xrightarrow{\sim} L \,:\, f \mapsto [2,f]$$

is an isomorphism of rings. However ε_1 need not be injective, in fact $[1,a] = [1,b]$ is true, iff $\varphi(a) = \varphi(b)$, so the injectivity of ε_1 stands or falls with the injectivity of φ.

(ii) If the index set I has a maximal element $m \in I$, that is $i \leq m$ for any $i \in I$, then the direct limit will be isomorphic to M_m. Hereby ε_m is a $\star$-morphism and its inverse morphism is given to be

$$\varinjlim (M_i,\, \mu_i^j) \xrightarrow{\sim} \,:\, [i,x] \mapsto \mu_i^m(x)$$

(3.171) Example: (viz. 776)
The following example will build up on *Shifting Ideals in polynomial Rings* in section 8.2. Consider any ascending chain of index sets $I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots$ and denote the union of all these sets by

$$I_\infty \;:=\; \bigcup_{n\in\mathbb{N}} I_n$$

Now, for any $n \in \mathbb{N}\cup\{\infty\}$ we abbreviate $R[n] := R[I_n] = R[t_i \mid i \in I_n]$ the polynomial ring in the variables t_i, where i runs in I_n. In particular, for any $m \leq n \in \mathbb{N}\cup\{\infty\}$ we have the canonical embeddings, which we will denote by

$$\iota_m^n \;:\; R[m] \;\hookrightarrow\; R[n] \;:\; f \mapsto f\,1_{R[n]}$$

Then $(R[n], \iota_m^n)$ is a directed system of rings over $\mathbb{N}$, and the direct limit of this system is isomorphic to $R[\infty]$, under the following isomorphism

$$\varinjlim (R[n],\, \iota_m^n) \;\xrightarrow{\sim}\; R[\infty] \;:\; [n,a] \mapsto \iota_n^\infty(a)$$

The inverse homomorphism is given to be $f \mapsto [n, \check{f}]$, where $n \in \mathbb{N}$ is taken in such a way that there is some $\check{f} \in R[n]$ satisfying $f = \iota_n^\infty(\check{f})$. This is possible, due to (8.15.(i)).

(3.172) Proposition: (viz. 777)
Let $(R,+,\cdot)$ be a commutative ring and (M_i, μ_i^j) be a direct system of R-modules over the net $(I,\leq)$. Denote its direct limit by M_∞ and let $\varepsilon_i : M_i \to M_\infty$ be the structural morphisms. Finally, for any $i \in I$, let $X_i \subseteq M_i$ be an arbitrary subset and denote

$$X_\infty \;:=\; \bigcup_{i\in I} \varepsilon_i(X_i) \quad\subseteq\quad M_\infty$$

(i) If for any $i \in I$ the set X_i generates M_i as an R-module, then X_∞ generates M_∞ as an R-module.

(ii) If (1) for any $i \in I$ the set X_i is R-linearly independent and (2) for any $i \leq j \in I$ we have $\mu_i^j(X_i) \subseteq X_j$, then X_∞ is R-linearly independent again.

(iii) If (1) for any $i \in I$ the set X_i is an R-basis of M_i and (2) for any $i \leq j \in I$ we have $\mu_i^j(X_i) \subseteq X_j$, then X_∞ is an R-basis of M_∞ again.

(3.173) Lemma: (viz. 778)

(i) *Universal Property of the inverse Limit*: Let (M_i, μ_i^j) be an inverse system of $\star$-objects over the partially ordered set $(I,\leq)$. Denote its inverse limit by M_∞ and let $\pi_i : M_\infty \to M_i$ be the canonical projections. Also consider a system (L, λ_i) satisfying the following properties

(1) L is a $\star$-object

(2) $\forall\, i \in I$ we get: $\lambda_i : L \to M_i$ is a $\star$-morphism

(3) $\forall\, i,j \in I$ with $i \leq j$ we get: $\lambda_i = \mu_j^i \lambda_j$

(4) Specifically in the case of topological spaces, we require $(I,\leq)$ to be a net.

Then there is a uniquely determined $\star$-morphism $\lambda : L \to M_\infty$ such that for any $i \in I$ we have the commutative diagram: $\lambda_i = \pi_i \lambda$ and this is given to be $\lambda(\ell) := (\mu_i(\ell))$.

(ii) *Universal Property of the direct Limit*: Let (M_i, μ_i^j) be a direct system of $\star$-objects over the net $(I, \leq)$. Denote its direct limit by M_∞ and let $\varepsilon_i : M_i \to M_\infty$ be the structure morphisms. Also consider a system (L, λ_i) satisfying the following properties

(1) L is a $\star$-object

(2) $\forall\, i \in I$ we get: $\lambda_i : M_i \to L$ is a $\star$-morphism

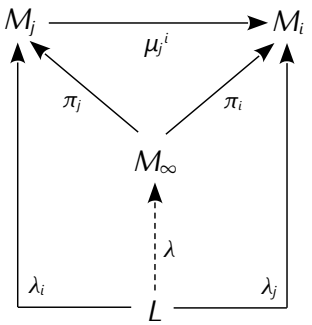
(3) $\forall\, i, j \in I$ with $i \leq j$ we get: $\lambda_i = \lambda_j \mu_i^j$

(4) Specifically in the case of topological spaces, we require a fourth property: For any i, $j \in I$ with $i \leq j$ we need the transition morphism μ_i^j to be an open map.

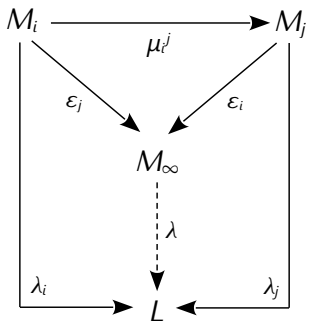
Then there is a uniquely determined $\star$-morphism $\lambda : M_\infty \to L$ such that for any $i \in I$ we have the commutative diagram: $\lambda_i = \lambda \varepsilon_i$ and this is given to be $\lambda([i, x]) := \mu_i(x)$.

(3.174) Remark:
The following diagrams depict the situation of the universal properties of the inverse resp. direct limits. A pair (L, φ_i) satisfying the respective properties (1) to (3) (even (4) for topological spaces) is occasionally said to be a *target*. Then by construction the inverse limit (M_∞, π_i) resp. the direct limit $(M_\infty, \varepsilon_i)$ are targets, themselves. The inverse limit is said to be an *attracting target*, whereas the direct limit is said to be a *repulsing target*. This refers to the direction of the morphism λ. And these notions stand to reason, if we take a look at the respective diagrams involved:

universal property of the inverse limit



universal property of the direct limit



(3.175) Corollary: (viz. 779)
This corollary holds for the following kinds $\star$-objects: Sets, commutative groups, commutative rings, any R-modules and commutative R-algebras (where as always $(R, +, \cdot)$ is any commutative ring). It need not hold true for non-commutative groups, rings and algebras or topological spaces.

(i) Let (M_i, μ_i^j) be an inverse system of $\star$-objects over the partially ordered set $(I, \leq)$ and fix another $\star$-object L, of the same kind. Then $H_i := \hom(L, M_i)$ is another $\star$-object, under the point-wise operations. And for any $i \leq j \in I$ we also get a $\star$-morphism, by

$$(\mu_j^i)_* \,:\, H_j \,\to\, H_i \,:\, \psi \,\mapsto\, \mu_i^j \psi$$

Thereby $(H_i, (\mu_j^i)_*)$ becomes an inverse system of $\star$-objects, over the same partially ordered set $(I, \leq)$. Let us abbreviate their inverse limits by

$$\begin{aligned} M_\infty &:= \varprojlim \left(M_i, \mu_j^i \right) \\ H_\infty &:= \varprojlim \left(H_i, (\mu_j^i)_* \right) \end{aligned}$$

As usual let $\pi_i : M_\infty \to M_i$ be the canonical projections of the inverse limit. Then we obtain a $\star$-isomorphism between the $\star$-homomorphisms from L to the inverse limit and the inverse limit of the $\star$-homomorphisms from L. And this isomorphism is given to be

$$\begin{array}{rcl} \hom(L, M_\infty) & \xrightarrow{\sim} & H_\infty \\ \psi & \mapsto & (\pi_i \psi) \\ (u \mapsto (\psi_i(u))) & \leftarrow\!\shortmid & (\psi_i) \end{array}$$

(ii) Let (M_i, μ_i^j) be a directed system of $\star$-objects over the net $(I, \leq)$ and fix another $\star$-object N, of the same kind. Then $H_i := \hom(M_i, N)$ is another $\star$-object, under the point-wise operations. And for any $i \leq j \in I$ we also get a $\star$-morphism, by

$$(\mu_i^j)^* \ : \ H_j \ \to \ H_i \ : \ \psi \mapsto \psi \mu_i^j$$

Thereby $(H_i, (\mu_i^j)^*)$ becomes another inverse system of $\star$-objects, over the same net $(I, \leq)$. Let us abbreviate their direct resp. inverse limits by

$$\begin{aligned} M_\infty &:= \varinjlim \left(M_i, \mu_i^j \right) \\ H_\infty &:= \varprojlim \left(H_i, (\mu_i^j)^* \right) \end{aligned}$$

As usual let $\varepsilon_i : M_i \to M_\infty$ be the structural morphisms of the direct limit. Then we obtain a $\star$-isomorphism between the $\star$-homomorphisms from the direct limit to N and the inverse limit of the $\star$-homomorphisms to N. And this isomorphism is given to be

$$\begin{array}{rcl} \hom(M_\infty, N) & \xrightarrow{\sim} & H_\infty \\ \psi & \mapsto & (\psi \varepsilon_i) \\ ([i, x] \mapsto \psi_i(x)) & \leftarrow\!\shortmid & (\psi_i) \end{array}$$

(3.176) Remark:
It will not have escaped your notice, that we only discussed two of the four possible combinations of homomorphisms and limits in (3.175). And in these two cases we took the indirect limit of the homomorphisms. If (M_i, φ_i^j) is a directed set of of $\star$-objects, then (by the universal property of the direct limit), we still find the following $\star$-morphism. Being a bit sloppy in our notation, we get

$$\varinjlim \hom(L, M_i) \ \to \ \hom(L, \varinjlim M_i) \ : \ [i, \psi] \ \mapsto \ \varepsilon_i \psi$$

where ε_i is the structural morphism of $\varinjlim M_i$ again. Alas, in general this $\star$-morphism need not be an isomorphism. In fact this is the case, if and only if L is finitely presented. Likewise, if (M_i, φ_j^i) is an inverse system of $\star$-objects, and π_i are the canonical projections of $\varprojlim M_i$, then (by the universal property of the direct limit), we find the following $\star$-morphism, again

$$\varinjlim \hom(M_i, N) \ \to \ \hom(\varprojlim M_i, N) \ : \ [i, \psi] \ \mapsto \ \psi\pi_i$$

(3.177) Definition: (viz. 781)

(i) Let (M_i, μ_j^i) and (N_i, ν_j^i) be inverse systems of $\star$-objects, over the same partially ordered set $(I, \leq)$ and let M_∞ and N_∞ be the respective inverse limits. Then an I-tuple (φ_i) is said to be **$\star$-system-morphism**, iff it satisfies both of the following properties

(1) For any $i \in I$ we find $\varphi_i : M_i \to N_i$ to be a $\star$-morphism

(2) For any $i \leq j \in I$ we have the commutative diagram $\varphi_i \mu_j^i = \nu_j^i \varphi_j$

In this case we find a $\star$-morphism $\varphi_\infty : M_\infty \to N_\infty$ by letting $(x_i) \mapsto (\varphi_i(x_i))$. And we denote this morphism by $\varprojlim (\varphi_i)$. For the $\star$-system-morphism itself, we will write

$$(\varphi_i) \ : \ (M_i, \mu_j^i) \ \to \ (N_i, \nu_j^i)$$

(ii) Let (M_i, μ_j^i) and (N_i, ν_j^i) be direct systems of $\star$-objects, over the same net $(I, \leq)$ and let M_∞ and N_∞ be the respective direct limits. Then an I-tuple (φ_i) is said to be **$\star$-system-morphism**, iff it satisfies both of the following properties (1) and (2)

(1) For any $i \in I$ we find $\varphi_i : M_i \to N_i$ to be a $\star$-morphism

(2) For any $i \leq j \in I$ we have the commutative diagram $\varphi_i \mu_j^i = \nu_j^i \varphi_j$

(3) Specifically in case of topological spaces, we also assume, that for any $i \leq j \in I$ the transition map $\nu_i^j : N_i \to N_j$ not only is continuous, but also is open.

In this case we find a well-defined $\star$-morphism $\varphi_\infty : M_\infty \to N_\infty$ by letting $[i, x] \mapsto [i, \varphi_i(x)]$. And we denote this morphism by $\varprojlim (\varphi_i)$. For the $\star$-system-morphism itself, we will write

$$(\varphi_i) \ : \ (M_i, \mu_i^j) \ \to \ (N_i, \nu_i^j)$$

(3.178) Proposition: (viz. 782)

(i) *Inverse limits of modules are left-exact*: Fix any commutative ring $(R, +, \cdot)$ and let (L_i, λ_j^i), (M_i, μ_j^i) and (N_i, ν_j^i) be inverse systems of R-modules over the same partially ordered set $(I, \leq)$. Also consider $(\varphi_i) : (L_i, \lambda_j^i) \to (M_i, \mu_j^i)$ and $(\psi_i) : (M_i, \mu_j^i) \to (N_i, \nu_j^i)$ two R-module-system homomorphisms, such that for any $i \in I$ the chains

$$0 \ \to \ L_i \ \xrightarrow{\varphi_i} \ M_i \ \xrightarrow{\psi_i} \ N_i$$

are exact. Let L_∞, M_∞ and N_∞ be the respective inverse limits of the inverse systems and let φ_∞ and ψ_∞ be the respective inverse limits of the morphisms, as in (3.177.(i)). Then we find, that the following chain is exact, as well:

$$0 \;\to\; L_\infty \;\xrightarrow{\varphi_\infty}\; M_\infty \;\xrightarrow{\psi_\infty}\; N_\infty$$

(ii) *Direct limits of modules are exact*: Fix any commutative ring $(R, +, \cdot)$ and let (L_i, λ_i^j), (M_i, μ_i^j) and (N_i, ν_i^j) be direct systems of R-modules over the same net $(I, \leq)$. Also consider two R-module-system homomorphisms $(\varphi_i) : (L_i, \lambda_i^j) \to (M_i, \mu_i^j)$ and $(\psi_i) : (M_i, \mu_i^j) \to (N_i, \nu_i^j)$, such that for any $i \in I$ the chains

$$0 \;\to\; L_i \;\xrightarrow{\varphi_i}\; M_i \;\xrightarrow{\psi_i}\; N_i \;\to\; 0$$

are exact. Let L_∞, M_∞ and N_∞ be the respective direct limits of the direct systems and let φ_∞ and ψ_∞ be the respective direct limits of the morphisms, as in (3.177.(ii)). Then we find, that the following chain is exact, as well:

$$0 \;\to\; L_\infty \;\xrightarrow{\varphi_\infty}\; M_\infty \;\xrightarrow{\psi_\infty}\; N_\infty \;\to\; 0$$

Pro: completion is exact Thm: spec of direct limit of rings is inverse limit of specs

Chapter 4

Linear Algebra

4.1 Matrix Algebra

Matrices serve two purposes: First of all they can represent systems of linear equations. And secondly (by fixing ordered bases) they can be used to represent homomorphisms between free modules. Using matrices these concepts are interlocked: The set of solutions is the kernel of the homomorphism (resp. an affine shift of the kernel in case of an inhomogeneous equation).
Also matrices provide a method of keeping track of the manipulations of a system of linear equations - the elementary matrices. Hence the algorithm how to solve a system of linear equations (Gauss-Algorithm) can be expressed in terms of matrices. This ultimately leads to a criterion whether a system of linear equations is (unambiguously) solvable - the determinant. So, as a first step, let us introduce the notion of a matrix and define a bunch of operations on matrices, that will be used later on.

(4.1) Definition:
Let $(R, +, \cdot)$ be any ring and fix a natural number $1 \leq n \in \mathbb{N}$. As before we will concern ourselves with the set R^n of n-tuples over R. Recall that this is given to be

$$R^n \;:=\; \{\, (x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in R \,\}$$

In linear algebra it is customary (and occasionally useful) to write the n-tuple $x = (x_1, \ldots, x_n)$ in vertical order as well, that is we use two ways of denoting an n-tuple

$$(x_1, \ldots, x_n) \;=\; \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

We already turned R^n into an R-algebra by establishing the point-wise operations on R^n, let us recall this: Given any $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in R^n$ and any $a \in R$ we have defined the operations

$$\begin{aligned} (x_1, \ldots, x_n) + (y_1, \ldots, y_n) &:= (x_1 + y_1, \ldots, x_n + y_n) \\ (x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) &:= (x_1 \cdot y_1, \ldots, x_n \cdot y_n) \\ a(x_1, \ldots, x_n) &:= (ax_1, \ldots, ax_n) \end{aligned}$$

As a new operation on R^n we define the **scalar product** (do not confuse this with the *scalar multiplication*) $R^n \times R^n \to R : (x,y) \mapsto \langle x,y\rangle$ which is defined to be (as always $x = (x_1,\dots,x_n)$ and $y = (y_1,\dots,y_n)$)

$$\langle x,y\rangle \;:=\; \sum_{i=1}^{n} x_i\, y_i$$

Finally we need to fix an easy notation for the canonical projections $\pi_i : R^n \to R : x \mapsto x_i$ of the product R^n. Recall that the π_i are R-algebra homomorphisms. Given any $i \in 1\dots n$ we denote

$$[x]_i \;:=\; x_i \quad \text{where} \quad x \;=\; (x_1,\dots,x_n)$$

(4.2) Remark:

(i) There are a multitude of ways how to embed $R \hookrightarrow R^n$ as a subalgebra. The most reasonable one (due to its symmetry) is to interpret $a \in R$ as the tuple $(a) = (a,\dots,a) \in R^n$. The advantage of this is evident: The multiplication then coincides with the scalar multiplication: That is we get $(a)\cdot x = ax$. Hence we fix

$$R \;\hookrightarrow\; R^n \;:\; a \mapsto (a) := (a,\dots,a)$$

(ii) Trivially R^n is a free module, having the Euclidean R-basis $\mathcal{E} = \{\, e_1,\dots,e_n \,\}$. Thereby the basis elements $e_j = (\delta_{i,j}) \in R^n$ are given to be (refer to (3.60) for more details)

$$\begin{aligned} e_1 &:= (1,0,0,\dots,0,0)\\ e_2 &:= (0,1,0,\dots,0,0)\\ &\;\;\vdots\\ e_n &:= (0,0,0,\dots,0,1) \end{aligned}$$

(iii) If R is a commutative ring, then clearly the scalar product on R^n has some neat computational properties: In fact it is a symmetric bilinear form of R^n: For any x, y, $z \in R^n$ and $a \in R$ we get

$$\begin{aligned} \langle ax+y,z\rangle &= a\langle x,z\rangle + \langle y,z\rangle \quad R\text{-linearity (in the 1st argument)}\\ \langle x,ay+z\rangle &= a\langle x,y\rangle + \langle y,z\rangle \quad R\text{-linearity (in the 2nd argument)}\\ \langle x,y\rangle &= \langle y,x\rangle \qquad\qquad \text{symmetry} \end{aligned}$$

In case R is not commutative only the R-linearity in the 1st argument is preserved. The other two properties are lost, in general. Prob all these properties are straightforward applications of the axioms of rings: $\langle ax+y,z\rangle = \sum_i (ax_i+y_i)z_i = \sum_i (ax_iz_i + y_iz_i) = a\sum_i x_iz_i + \sum_i y_iz_i = a\langle x,z\rangle + \langle y,z\rangle$. And the R-linearity in the second argument can be proved in complete analogy. The symmetry of the scalar product is evident: $\langle x,y\rangle = \sum_i x_iy_i = \sum_i y_ix_i = \langle y,x\rangle$.

(iv) Note that in general there is a difference between the scalar product $\langle x, y\rangle$ and an *inner product* $\langle x \mid y\rangle$. The latter will be defined in the case of $R = \mathbb{C}$ only and there is a subtle distinction between the scalar and inner products - the inner products uses complex conjugates. However this difference has far-reaching consequences: In contrast to the inner product, the scalar product over $R = \mathbb{C}$ is *not* positively definite. In fact we see that

$$\langle \begin{pmatrix} 1 \\ i \end{pmatrix}, \begin{pmatrix} 1 \\ i \end{pmatrix} \rangle \;=\; 1^2 + i^2 \;=\; 1 - 1 \;=\; 0$$

(4.3) Definition:
Let $(R, +, \cdot)$ be any ring again and fix two natural numbers $1 \leq m, n \in \mathbb{N}$. Then a $(m \times n)$-**matrix** is defined to be an n-tuple of m-tuples over R. Formally we will denote this set, by

$$\mathrm{mat}_{m,n}(R) \;:=\; (R^m)^n$$

A matrix usually is written as an m times n block of elements of R. That is if we have a number of n m-tuples $a_j = (a_{1,j}, \ldots, a_{m,j}) \in R^m$ where $j \in 1 \ldots n$ then we write the matrix $A = (a_1, \ldots, a_n)$ in the following form

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix} \;:=\; (a_{i,j}) \;:=\; A$$

That is the second index j of $A = (a_{i,j})$ designates the jth m-tuple a_j of A and this is written as the jth column of A. Complementary the first index i of $A = (a_{i,j})$ designates the ith component within the m-tuple a_j and these are written as the ith row of A.

We will later introduce some binary operations on matrices. To this end we need to introduce formal notations: Fix the $(m \times n)$-matrix $A = (a_{i,j})$ as above. Then - for any $i \in 1 \ldots n$ and any $j \in 1 \ldots n$ - we denote the (i, j)th **entry** of A, the i-th **row** of A and the j-th **column** of A respectively by

$$\begin{aligned} \mathrm{ent}_{i,j}(A) &:= a_{i,j} \in R \\ \mathrm{row}_i(A) &:= (a_{i,1}, a_{i,2}, \ldots, a_{i,n}) \in R^n \\ \mathrm{col}_j(A) &:= (a_{1,j}, a_{2,j}, \ldots, a_{m,j}) \in R^m \end{aligned}$$

Analogous to our notation for tuples we also denote $[A]_{i,j} := \mathrm{ent}_{i,j}(A) = a_{i,j}$. The **transpose** A^* of an $(m \times n)$-matrix $A = (a_{i,j})$ is defined to be the $(n \times m)$-matrix in which columns and rows are interchanged

$$A^* \;:=\; \begin{pmatrix} a_{1,1} & a_{2,1} & \cdots & a_{m,1} \\ a_{1,2} & a_{2,2} & \cdots & a_{m,2} \\ \vdots & \vdots & & \vdots \\ a_{1,n} & a_{2,n} & \cdots & a_{m,n} \end{pmatrix} \;\in\; \mathrm{mat}_{n,m}(R)$$

If $m = n$ then the rectangular block A of elements becomes a **square**. As this is an important special case we abbreviate our notation somewhat:

$$\mathsf{mat}_n(R) \;:=\; \mathsf{mat}_{n,n}(R) \;=\; (R^n)^n$$

A special case of such a matrix is a **diagonal matrix**. That is a square matrix $A = (a_{i,j})$ in which all entries off the diagonal are zero, i.e. $a_{i,j} = 0$ for any $i \neq j \in 1 \ldots n$. And if we are given n-elements $a_1, \ldots, a_n \in R$ then the diagonal matrix with the entries a_i on its diagonal is denoted by

$$\mathsf{dia}(a_1, \ldots, a_n) \;:=\; \begin{pmatrix} a_1 & 0 & \cdots & 0 & 0 \\ 0 & a_2 & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & & a_{n-1} & 0 \\ 0 & 0 & \cdots & 0 & a_n \end{pmatrix} \;\in\; \mathsf{mat}_n(R)$$

If $A \in \mathsf{mat}_n(R)$ is any square matrix, then we introduce the **trace** of A to be the sum of all its entries on the main diagonal, formally

$$\mathsf{tr}(A) \;:=\; \sum_{i=1}^{n} \mathsf{ent}_{i,i}(A)$$

For completeness purposes let us finally introduce a notation for the set of matrices of any size over R

$$\mathsf{Mat}(R) \;:=\; \bigcup_{m=1}^{\infty} \bigcup_{m=1}^{\infty} \mathsf{mat}_{m,n}(R)$$

(4.4) Remark:

(i) By construction an n-tuple $x = (x_1, x_2, \ldots, x_n) \in R^n$ is an $(n \times 1)$-matrix (which is sometimes also called a *column-vector*) which we denote by

$$x \;=\; \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \;\in\; \mathsf{mat}_{n,1}(R) \;=\; R^n$$

So n-tuples and and $(n \times 1)$-matrices really are the same thing, which is why it is perfectly legitimate to write tuples as column-vectors. The transpose x^* of x thereby is an $(1 \times n)$-matrix (which is sometimes called a *row-vector*)

$$x^* \;=\; \begin{pmatrix} x_1 & x_2 & \ldots & x_n \end{pmatrix} \;\in\; \mathsf{mat}_{1,n}(R)$$

Note that the row-vector is *not* the n-tuple $(x_1, x_2, \ldots, x_n)$ anymore! From an abstract point of view, it is an element of the dual-space of R^n (i.e. it is a linear map of the form $R^n \to R$). From a notational point of view it misses the commas, we use in tuples.

(ii) By definition of a $(m \times n)$-matrix, every n m-tuples $a_j = (a_{i,j}) \in R^m$ (where $j \in 1 \dots n$) determine a matrix $A := (a_1, \dots, a_n)$. To stress, that the a_j build up the columns of A we write

$$\begin{pmatrix} | & & | \\ a_1 & \cdots & a_n \\ | & & | \end{pmatrix} := (a_{i,j})$$

Conversely, if we are given m n-tuples $a_i = (a_{i,j}) \in R^n$ (where $i \in 1 \dots m$) we can build up a $(m \times n)$-matrix $A = (a_{i,j})$ by taking the a_i to be the rows of A. In this case we write

$$\begin{pmatrix} — & a_1 & — \\ & \vdots & \\ — & a_m & — \end{pmatrix} := (a_{i,j})$$

(ii) Recall that an $(m \times n)$-matrix $A = (a_{i,j})$ is defined to be an n-tuple of m-tuples of R. And the (i,j)th entry $a_{i,j}$ of A is the ith component of the jth component of A. So in a formal way that is

$$[A]_{i,j} = a_{i,j} = [[A]_j]_i$$

(4.5) Definition:
Let $(R, +, \cdot)$ be any ring again and consider the natural numbers $1 \leq m$ and $n \in \mathbb{N}$. By construction the set $\mathrm{mat}_{m,n}(R)$ of $(m \times n)$-matrices of R forms an R-module under the point-wise operations. That is: consider $a \in R$ and two $(m \times n)$-matrices $A = (a_{i,j})$ and $B = (b_{i,j}) \in \mathrm{mat}_{m,n}(R)$. Then we define the **addition** and **scalar-multiplication**

$$\begin{aligned} A + B &:= (a_{i,j} + b_{i,j}) \\ aB &:= (a\, b_{i,j}) \end{aligned}$$

Now consider another natural number $1 \leq l \in \mathbb{N}$ and suppose that $A \in \mathrm{mat}_{l,m}(R)$ is a $(l \times m)$-matrix, whereas $B \in \mathrm{mat}_{m,n}(R)$ is an $(m \times n)$-matrix. Then we can define the **matrix-multiplication** AB of A and B to be the following $(l \times n)$-matrix

$$AB := \Big(\langle \mathrm{row}_i(A), \mathrm{col}_k(B) \rangle\Big) = \left(\sum_{j=1}^{m} a_{i,j}\, b_{j,k}\right) \in \mathrm{mat}_{l,n}(R)$$

That is the (i,k)-th entry of AB is the i-th row of A multiplied with the k-th column of B. That is: If $a_i = \mathrm{row}_i(A) = (a_{i,1}, \dots, a_{i,m})$ is the i-th row of A and $b_k = \mathrm{col}_k(B) = (b_{1,k}, \dots, b_{m,k})$ is the k-th column of B, then the matrix-multiplication follows the scheme

$$\begin{pmatrix} — & a_1 & — \\ & \vdots & \\ — & a_l & — \end{pmatrix} \begin{pmatrix} | & & | \\ b_1 & \cdots & b_n \\ | & & | \end{pmatrix} = \Big(\langle a_i, b_k \rangle\Big)$$

A special case of this is the **matrix-vector** multiplication: Given an $(m \times n)$-matrix $A \in \mathrm{mat}_{m,n}(R)$ and an n-tuple $x \in R^n$ over R we obtain an m-tuple $Ax \in R^m$ by virtue of

$$Ax \;:=\; (\langle \mathrm{row}_1(A), x\rangle, \ldots, \langle \mathrm{row}_m(A), x\rangle) \;\in\; R^m$$

That is we use the rows of A to be multiplied with the tuple x. So if $a_i = \mathrm{row}_i(A) = (a_{i,1}, \ldots, a_{i,n})$ is the i-th row of A, then the matrix-vector multiplication can be pinned down in the more intuitive way

$$\begin{pmatrix} \text{—} & a_1 & \text{—} \\ & \vdots & \\ \text{—} & a_m & \text{—} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \;=\; \begin{pmatrix} \langle a_1, x\rangle \\ \vdots \\ \langle a_n, x\rangle \end{pmatrix} \;\in\; R^m$$

(4.6) Remark:

(i) Let us reformulate the above definitions of addition, scalar multiplication and vector multiplication in terms of the entries of the resulting matrices. That is we take A, $B \in \mathrm{mat}_{m,n}(R)$, $a \in R$ and $x \in R^n$. Then for any $i \in 1 \ldots m$ and any $j \in 1 \ldots n$ we have

$$\begin{aligned} \mathrm{ent}_{i,j}(aA + B) &= a\,\mathrm{ent}_{i,j}(A) + \mathrm{ent}_{i,j}(B) \\ [Ax]_i &= \sum_{j=1}^{n} \mathrm{ent}_{i,j}(A)\;[x]_j \end{aligned}$$

And if $A \in \mathrm{mat}_{l,m}(R)$ and $B \in \mathrm{mat}_{m,n}(R)$ we can also reformulate the matrix multiplication for all the entries $i \in 1 \ldots l$ and $k \in 1 \ldots n$

$$\mathrm{ent}_{i,k}(AB) \;=\; \sum_{j=1}^{m} \mathrm{ent}_{i,j}(A)\,\mathrm{ent}_{j,k}(B)$$

(ii) If $x = (x_1, x_2, \ldots x_n)$ and $y = (y_1, y_2, \ldots y_n) \in R^n$ are n-tuples over R, then the matrix multiplication can be used to emulate the scalar product

$$x^* y \;=\; \sum_{j=1}^{n} x_j y_j \;=\; \langle x, y\rangle$$

(iii) If $A \in \mathrm{mat}_{m,n}(R)$ is an $(m \times n)$-matrix and $x = (x_1, x_2, \ldots, x_n) \in R^n$ is an n-tuple, then the matrix-vector multiplication yields the following linear combination of the columns of A

$$Ax \;=\; \sum_{j=1}^{n} \mathrm{col}_j(A) \cdot x_j \;\in\; R^m$$

Likewise, if $y = (y_1, y_2, \ldots, y_m) \in R^m$ is an m-tuple, then the matrix multiplication can also yield the following linear combination of the rows of A

$$y^* A \;=\; \sum_{i=1}^{m} y_i \cdot \mathrm{row}_i(A) \;\in\; R^n$$

(iv) Let us also reformulate the transposition $A \mapsto A^*$ of matrices in terms of the rows, columns and entries. Then it is clear that for any $A \in \mathrm{mat}_{m,n}(R)$ and any $i \in 1 \ldots m$, $j \in 1 \ldots n$ we get

$$\begin{aligned} \mathrm{ent}_{j,i}(A^*) &= \mathrm{ent}_{i,j}(A) \\ \mathrm{col}_i(A^*) &= \mathrm{row}_i(A) \\ \mathrm{row}_j(A^*) &= \mathrm{col}_j(A) \end{aligned}$$

Prob recall that $\mathrm{ent}_{j,i}(A^*) = \mathrm{ent}_{i,j}(A)$ is just the definition of the transpose A^*. And thus we find $\mathrm{col}_i(A^*) = (\mathrm{ent}_{1,i}(A^*), \ldots, \mathrm{ent}_{n,i}(A^*)) = (\mathrm{ent}_{i,1}(A), \ldots, \mathrm{ent}_{i,n}(A)) = \mathrm{row}_i(A)$. Likewise we compute $\mathrm{row}_j(A^*) = (\mathrm{ent}_{j,1}(A^*), \ldots, \mathrm{ent}_{j,m}(A^*)) = (\mathrm{ent}_{1,j}(A), \ldots, \mathrm{ent}_{m,j}(A)) = \mathrm{col}_j(A)$.

(v) If R is a commutative ring and $A \in \mathrm{mat}_{m,n}(R)$ is a matrix, then A gives rise to an R-module homomorphism of the following form, by vector-matrix multiplication

$$\varphi_A \ : \ R^n \to R^m \ : \ x \mapsto Ax$$

By abuse of notation we usually identify $\varphi_A = A$ here, but we will also see that all homomorphisms between finitely generated, free R-modules can be represented in this way - this will be the topic of section 4.4. Due to (iii) above the image of φ_A is generated by the columns of A, that is

$$\mathrm{im} \begin{pmatrix} | & & | \\ c_1 & \cdots & c_n \\ | & & | \end{pmatrix} \ = \ \mathrm{Lh}\{ c_1, \ldots, c_n \} \quad \leq_{\mathtt{m}} \quad R^m$$

Prob in a commutative ring R the scalar product $x \mapsto \langle r, x \rangle$ is R-linear for any $r \in R^n$, in particular for $r = \mathrm{row}_i(A)$. And as $x \mapsto Ax$ is the cartesian product of m-scalar products, φ_A is R-linear, too. Also, if $c_j := \mathrm{col}_j(A)$ is the j-th column of A, then we have $Ax = x_1c_1 + \ldots x_nc_n$ by (iii). That is the image of φ_A is precisely the linear hull of the c_j where $j \in 1 \ldots n$.

(vi) Note that the matrix-matrix multiplication AB is nothing but a matrix-vector multiplication Ab_k for all the column vectors b_k of B. I.e. given $A \in \mathrm{mat}_{l,m}(R)$ and $b_k \in R^m$ (where $k \in 1 \ldots n$) we have

$$A \begin{pmatrix} | & & | \\ b_1 & \cdots & b_m \\ | & & | \end{pmatrix} \ = \ \begin{pmatrix} | & & | \\ Ab_1 & \cdots & Ab_m \\ | & & | \end{pmatrix}$$

(vii) Suppose R is a commutative ring again and consider $A = \mathrm{mat}_{k,m}(R)$ and $B \in \mathrm{mat}_{m,n}(R)$. If for $i \in 1 \ldots k$ the i-th row of A is abbreviated by $a_i = \mathrm{row}_i(A) \in R^m$, then we can also rewrite a multiplication of B from the right as an operation of the transpose B^* on the rows of A

$$\begin{pmatrix} \text{---} & a_1 & \text{---} \\ & \vdots & \\ \text{---} & a_k & \text{---} \end{pmatrix} B \ = \ \begin{pmatrix} \text{---} & B^*a_1 & \text{---} \\ & \vdots & \\ \text{---} & B^*a_k & \text{---} \end{pmatrix}$$

Prob For any $r \in 1 \dots k$ and any $s \in 1 \dots n$ let us evaluate the (r,s)-entry of the matrix AB. By definition this is $[AB]_{r,s} = \langle a_i, \mathrm{col}_k(B) \rangle = \sum_j a_{r,j} b_{j,k}$. On the right hand side the (r,s)-th entry is the s-th component of $B^* a_r$ and hence $[B^* a_r]_s = \sum_j b^*_{s,j} [a_r]_j = \sum_j b_{j,s} a_{r,j}$. Since R is commutative both are equal.

(4.7) Example:
Let us take the integers $R = \mathbb{Z}$ as a base ring. Then we want to give an explicit example of a matrix multiplication, where $A \in \mathrm{mat}_{3,4}(\mathbb{Z})$ and $B \in \mathrm{mat}_{4,2}(\mathbb{Z})$ such that $AB \in \mathrm{mat}_{3,2}(\mathbb{Z})$. Our example will be

$$AB \;=\; \begin{pmatrix} -2 & 6 & 0 & 2 \\ 0 & 1 & 0 & 0 \\ 1 & 4 & 2 & -6 \end{pmatrix} \begin{pmatrix} 4 & 0 \\ -1 & 0 \\ 3 & 1 \\ 7 & 0 \end{pmatrix}$$

For the upper left entry of AB we compute $-2 \cdot 4 + 6 \cdot (-1) + 0 \cdot 3 + 2 \cdot 7 = 0$. Likewise for the lower left entry of AB (that is the third row and first column) we compute $1 \cdot 4 + 4 \cdot (-1) + 2 \cdot 3 - 6 \cdot 7 = -36$. Altogether we find

$$AB \;=\; \begin{pmatrix} 0 & 0 \\ -1 & 0 \\ -36 & 2 \end{pmatrix}$$

We installed some noteworthy specialities in this example: First of all we see that $\mathrm{col}_2(B) = e_3 \in \mathbb{Z}^4$. And this explains why the the second column of AB is just a copy of the third column of A

$$\mathrm{col}_2(AB) \;=\; A\,\mathrm{col}_2(B) \;=\; A\,e_3 \;=\; \mathrm{col}_3(A)$$

Likewise we have $\mathrm{row}_2(A) = e_2 \in \mathbb{Z}^4$ and that's why the the second row of AB is just another copy of the second row of B, since

$$\mathrm{row}_2(AB) \;=\; B^*\,\mathrm{row}_2(A) \;=\; B^*\,e_2 \;=\; \mathrm{col}_2(B^*) \;=\; \mathrm{row}_2(B)$$

And lastly we see that AB has an entire zero-row $\mathrm{row}_1(AB) = 0$. E.g. for the $(1,2)$-entry (= upper left) of AB this means that

$$\mathrm{ent}_{1,2}(AB) \;=\; \langle \mathrm{row}_1(A), \mathrm{col}_2(B) \rangle \;=\; 0$$

Geometrically speaking this means that $\mathrm{row}_1(A)$ and $\mathrm{col}_2(B) \in \mathbb{Z}^4$ are perpendicular. But this also warns us, that the product AB may vanish, even if A and B are non-zero.

(4.8) Proposition: (viz. 1013)
Consider any ring $(R, +, \cdot)$ and fix the natural numbers $1 \leq l$, m, n, p and $q \in \mathbb{N}$. Then all of the following statements hold true

(i) The set $\mathrm{mat}_{m,n}(R)$ of $(m \times n)$-matrices over R is an R-module under the addition and scalar multiplication of matrices, as defined in (4.5). The zero-element thereby is the *zero-matrix*

$$0 \;=\; (0) \;=\; \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

In fact $\mathrm{mat}_{m,n}(R)$ is a free R-module of rank mn. We can easily provide the *Euclidean* R-basis $\mathcal{E} := \{ E_{r,s} \mid r \in 1 \ldots m, s \in 1 \ldots n \}$ of $\mathrm{mat}_{m,n}(R)$. Thereby $E_{r,s}$ is the $(m \times n)$ matrix that is entirely 0, except its (r,s)th entry, which is 1. Formally

$$E_{r,s} \;:=\; \left(\delta_{i,r}\, \delta_{j,s}\right) \;\in\; \mathrm{mat}_{m,n}(R)$$

(ii) The multiplication of matrices is associative and distributive (but in general not commutative). Suppose that A, B and C are matrices of compatible sizes, then

$$\begin{aligned} (AB)C &= A(BC) \\ A(B+C) &= AB + AC \\ (A+B)C &= AC + BC \end{aligned}$$

Note: to be of compatible sizes means $A \in \mathrm{mat}_{m,n}(R)$, $B \in \mathrm{mat}_{n,p}(R)$ and $C \in \mathrm{mat}_{p,q}(R)$ for the associativity, $A \in \mathrm{mat}_{l,m}(R)$, B and $C \in \mathrm{mat}_{m,n}(R)$ for the left-distributivity and A, $B \in \mathrm{mat}_{l,m}(R)$ and $C \in \mathrm{mat}_{m,n}(R)$ for the right-distributivity.

(iii) In particular the set $\mathrm{mat}_n(R)$ of $(n \times n)$-matrices over R is an R-algebra under the addition, scalar-multiplication and matrix-multiplication of matrices as defined in (4.5). Its unit-element is the *identity-matrix*

$$\mathbb{1}_n \;=\; (\delta_{i,j}) \;=\; \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & & 1 \end{pmatrix}$$

(iv) In particular - according to (iii) - $\mathrm{mat}_n(R)$ is a ring, however it need not be commutative, even if R is commutative. An invertible element of this ring is said to be an **invertible matrix**. I.e. $A \in \mathrm{mat}_n(R)$ is invertible iff there is some $B \in \mathrm{mat}_n(R)$ such that

$$AB \;=\; \mathbb{1}_n \;=\; BA$$

And in this case B is uniquely determined by A (as this is true for any ring) and (as in general rings before) we denote the **inverse matrix** of A by $A^{-1} := B$.

(v) Recall the definition of the center $\mathrm{cen}(R)$ of a ring R to be the sub-ring of all elements that commute with all other elements, that is $\mathrm{cen}(R) = \{\, a \in R \mid \forall\, b \in R : ab = ba \,\}$. Then the center of $\mathrm{mat}_n(R)$ is just the center of R embedded as diagonal matrices $\mathrm{cen}\left(\mathrm{mat}_n(R)\right) = \mathrm{cen}(R)\mathbb{1}_n$ or more explicitly:

$$\mathrm{cen}\left(\mathrm{mat}_n(R)\right) \;=\; \left\{ \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & a & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & & a \end{pmatrix} \;\middle|\; a \in \mathrm{cen}(R) \right\}$$

(vi) If R is a commutative ring and A, $B \in \mathrm{mat}_n(R)$ are square matrices over R, then the trace is invariant under commuting A and B

$$\mathrm{tr}(AB) \;=\; \mathrm{tr}(BA)$$

(vii) If R is a commutative ring, then any matrix $A \in \mathrm{mat}_{m,n}(R)$ induces a homomorphism of R-modules $\varphi_A : R^n \to R^n$ by using the matrix-vector multiplication $\varphi_A(x) := Ax$. And thereby we find the following, well-defined, isomorphism of R-modules

$$\mathrm{mat}_{m,n}(R) \;\xrightarrow{\sim}\; \mathrm{mhom}(R^n, R^m) \;:\; A \;\mapsto\; \varphi_A$$

(viii) The transposition $A \mapsto A^*$ of matrices is an isomorphism of R-modules $\mathrm{mat}_{m,n}(R) \xrightarrow{\sim} \mathrm{mat}_{n,m}(R)$. In particular for any $a \in R$ and any A, $B \in \mathrm{mat}_{m,n}(R)$ we have

$$(aA + B)^* \;=\; aA^* + B^*$$

(ix) If R is commutative, then the transposition of matrices swaps the order of matrix-multiplications. That is given any matrices $A \in \mathrm{mat}_{l,m}(R)$ and $B \in \mathrm{mat}_{m,n}(R)$ we find that

$$(AB)^* \;=\; B^*A^*$$

(ix) If R is commutative then taking inverses in $\mathrm{mat}_n(R)$ commutes with the transposition. To be precise: If $A \in \mathrm{mat}_n(R)$ is a square matrix, then A is invertible, if and only if A^* is invertible. And in this case the inverse of A^* is given to be

$$(A^*)^{-1} \;=\; \left(A^{-1}\right)^*$$

(xi) If R is a commutative ring, then for any vectors $x \in R^n$, $y \in R^m$ and any matrix $A \in \mathrm{mat}_{m,n}(R)$ we get the following identity in R

$$\langle Ax, y \rangle \;=\; \langle x, A^*y \rangle$$

(4.9) Definition: Block Notation

Let $(R, +, \cdot)$ be any ring, $1 \leq r, s \in \mathbb{N}$ and for any $p \in 1 \dots r$ consider some $1 \leq m(p) \in \mathbb{N}$. Likewise for any $q \in 1 \dots s$ let $1 \leq n(q) \in \mathbb{N}$, as well. Finally consider a matrix $A^{p,q} \in \mathrm{mat}_{m(p),n(q)}(R)$ for any $p \in 1 \dots r$ and $q \in 1 \dots s$. Now denote $m := m(1) + m(2) + \dots + m(r)$ and $n := n(1) + n(2) + \dots n(s)$. Then we define the **block matrix**

$$\begin{pmatrix} A^{1,1} & A^{1,2} & \dots & A^{1,s} \\ A^{2,1} & A^{2,2} & \dots & A^{2,s} \\ \vdots & \vdots & & \vdots \\ A^{r,1} & A^{r,2} & \dots & A^{r,s} \end{pmatrix} \in \mathrm{mat}_{m,n}(R)$$

in the following way: For any $p \in 1 \dots r$ and any $q \in 1 \dots s$ let $A^{p,q}$ have the entries $A^{p,q} = (a^{p,q}_{i,j})$ where $i \in 1 \dots m(p)$ and $j \in 1 \dots n(q)$. Then the above block matrix is set to be:

$$\begin{pmatrix}
a^{1,1}_{1,1} & \dots & a^{1,1}_{1,n(1)} & a^{1,2}_{1,1} & \dots & a^{1,2}_{1,n(2)} & \dots & a^{1,s}_{1,1} & \dots & a^{1,s}_{1,n(s)} \\
\vdots & & \vdots & \vdots & & \vdots & & \vdots & & \vdots \\
a^{1,1}_{m(1),1} & \dots & a^{1,1}_{m(1),n(1)} & a^{1,2}_{m(1),1} & \dots & a^{1,2}_{m(1),n(2)} & \dots & a^{1,s}_{m(1),1} & \dots & a^{1,s}_{m(1),n(s)} \\
a^{2,1}_{1,1} & \dots & a^{2,1}_{1,n(1)} & a^{2,2}_{1,1} & \dots & a^{2,2}_{1,n(2)} & \dots & a^{2,s}_{1,1} & \dots & a^{2,s}_{,n(s)} \\
\vdots & & \vdots & \vdots & & \vdots & & \vdots & & \vdots \\
a^{2,1}_{m(2),1} & \dots & a^{2,1}_{m(2),n(1)} & a^{2,2}_{m(2),1} & \dots & a^{2,2}_{m(2),n(2)} & \dots & a^{2,s}_{m(2),1} & \dots & a^{2,s}_{m(2),n(s)} \\
\vdots & & \vdots & \vdots & & \vdots & & \vdots & & \vdots \\
a^{r,1}_{1,1} & \dots & a^{r,1}_{1,n(1)} & a^{r,2}_{1,1} & \dots & a^{r,2}_{1,n(2)} & \dots & a^{r,s}_{1,1} & \dots & a^{r,s}_{1,n(s)} \\
\vdots & & \vdots & \vdots & & \vdots & & \vdots & & \vdots \\
a^{r,1}_{m(r),1} & \dots & a^{r,1}_{m(r),n(1)} & a^{r,2}_{m(r),1} & \dots & a^{r,2}_{m(r),n(2)} & \dots & a^{r,s}_{m(r),1} & \dots & a^{r,s}_{m(r),n(s)}
\end{pmatrix}$$

An important special case is the following: Given $A = (a_{i,j}) \in \mathrm{mat}_{k,l}(R)$ and $B = (b_{i,j}) \in \mathrm{mat}_{m,n}(R)$ matrices of arbitrary size $1 \leq k, l, m$ and $n \in \mathbb{N}$. Then we define the **direct sum** of these to be the following $(k+m) \times (l+n)$ matrix over R: Let $0_{k,n} = 0 \in \mathrm{mat}_{k,n}(R)$ and $0_{m,l} = 0 \in \mathrm{mat}_{m,l}(R)$ be the zero-matrices of the respective size, then

$$A \oplus B := \begin{pmatrix} A & 0_{k,n} \\ 0_{m,l} & B \end{pmatrix} \in \mathrm{mat}_{k+m,l+n}(R)$$

Explicitly $A \oplus B$ can be written out in the entries of A and B as we did above. In this form $A \oplus B$ is just the following matrix

$$A \oplus B = \begin{pmatrix}
a_{1,1} & a_{1,2} & \dots & a_{1,l} & 0 & 0 & \dots & 0 \\
a_{2,1} & a_{2,2} & \dots & a_{2,l} & 0 & 0 & \dots & 0 \\
\vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\
a_{k,1} & a_{k,2} & \dots & a_{k,l} & 0 & 0 & \dots & 0 \\
0 & 0 & \dots & 0 & b_{1,1} & b_{1,2} & \dots & b_{1,n} \\
0 & 0 & \dots & 0 & b_{2,1} & b_{2,2} & \dots & b_{2,n} \\
\vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\
0 & 0 & \dots & 0 & b_{m,1} & b_{m,2} & \dots & b_{m,n}
\end{pmatrix}$$

In a more formal way, suitable for programming and maybe for explicit computations, the entries of the direct sum $A \oplus B$ of the matrices A and B can be given to be the following

$$A \oplus B \;=\; \Big(s_{i,j}\Big)_{\substack{i\in 1\ldots k+m\\ j\in 1\ldots l+n}} \text{ where } s_{i,j} := \begin{cases} a_{i,j} \text{ if } i \leq k \text{ and } j \leq l \\ b_{i-k,j-l} \text{ if } i > k \text{ and } j > l \\ 0 \text{ if else} \end{cases}$$

(4.10) Remark: (viz. 1017)
If you concentrate a little, you will see, that this block-notation agrees with the matrix multiplication, in the following sense: Let $(R, +, \cdot)$ be a ring and $1 \leq r, s, t \in \mathbb{N}$. We assume the following block matrices to be of compatible structure

$$A \;=\; \begin{pmatrix} A^{1,1} & A^{1,2} & \ldots & A^{1,s} \\ A^{2,1} & A^{2,2} & \ldots & A^{2,s} \\ \vdots & \vdots & & \vdots \\ A^{r,1} & A^{r,2} & \ldots & A^{r,s} \end{pmatrix} \;\in\; \mathrm{mat}_{l,m}(R)$$

$$B \;=\; \begin{pmatrix} B^{1,1} & B^{1,2} & \ldots & B^{1,t} \\ B^{2,1} & B^{2,2} & \ldots & B^{2,t} \\ \vdots & \vdots & & \vdots \\ B^{s,1} & B^{s,2} & \ldots & B^{s,t} \end{pmatrix} \;\in\; \mathrm{mat}_{m,n}(R)$$

That is $A^{i,j}$ is a $(l(i) \times m(j))$-matrix over R and $B^{j,k}$ is a $(m(j) \times n(k))$-matrix over R for the same $m(j)$. In other words the vertical borders in A are of the same sizes, as the horizontal borders of B. Then the product AB can be computed using the usual multiplication of matrices

$$AB \;=\; \begin{pmatrix} \sum_{j=1}^{s} A^{1,j}B^{j,1} & \ldots \sum_{j=1}^{s} A^{1,j}B^{j,t} \\ \vdots & \vdots \\ \sum_{j=1}^{s} A^{r,j}B^{j,1} & \ldots \sum_{j=1}^{s} A^{r,j}B^{j,1} \end{pmatrix} \;\in\; \mathrm{mat}_{l,n}(R)$$

This becomes clear, once you realize, that the u-th row of A and v-th column of B break down into a row u' along the sub-matrices $A^{i,j}$ and the v'-column along the sub-matrices $B^{j,k}$ where j runs from 1 to s. Hence the scalar product $\langle \mathrm{row}_u(A), \mathrm{col}_v(B)\rangle$ breaks down into the sum of s scalar products $\langle \mathrm{row}_{u'}(A^{i,j}), \mathrm{col}_{v'}(B^{j,k})\rangle$. Refer to the proof for details. In particular we have the following product of block matrices that is mostly used, when $A^{2,1} = 0$

$$\begin{pmatrix} A^{1,1} & A^{1,2} \\ A^{2,1} & A^{2,2} \end{pmatrix} \begin{pmatrix} B^{1,1} & B^{1,2} \\ B^{2,1} & B^{2,2} \end{pmatrix} \;=\; \begin{pmatrix} A^{1,1}B^{1,1} + A^{1,2}B^{2,1} & A^{1,1}B^{1,2} + A^{1,2}B^{2,2} \\ A^{2,1}B^{1,1} + A^{2,2}B^{2,1} & A^{2,1}B^{1,2} + A^{2,2}B^{2,2} \end{pmatrix}$$

(4.11) Corollary:
Let $(R,+,\cdot)$ be any ring, $1 \leq n \in \mathbb{N}$ and $e_k \in R^n$ be the Euclidean basis vectors again, i,e, $e_k = (\delta_{i,k})$. If now $A \in \mathrm{mat}_n(R)$ is an invertible matrix, then the columns of the inverse matrix A^{-1} are uniquely determined by the property $A\,\mathrm{col}_k(A^{-1}) = e_k$. That is, if for any $k \in 1 \ldots n$ the vector $x_k \in R^k$ is the solution of $Ax_k = e_k$, then

$$A^{-1} \;=\; \begin{pmatrix} | & & | \\ x_1 & \cdots & x_n \\ | & & | \end{pmatrix}$$

Prob Let $x_k := A^{-1}e_k$ then $Ax_k = AA^{-1}e_k = \mathbb{1}_n e_k = e_k$, i.e. x_k is the solution of $Ax_k = e_k$. Then by (4.6.(v)) A^{-1} maps the columns of $\mathbb{1}_n$ onto x_1 to x_n, that is we get the identity

$$A^{-1} \;=\; A^{-1}\mathbb{1}_n \;=\; A^{-1}\begin{pmatrix} | & & | \\ e_1 & \cdots & e_n \\ | & & | \end{pmatrix} \;=\; \begin{pmatrix} | & & | \\ A^{-1}e_1 & \cdots & A^{-1}e_n \\ | & & | \end{pmatrix} \;=\; \begin{pmatrix} | & & | \\ x_1 & \cdots & x_n \\ | & & | \end{pmatrix}$$

(4.12) Remark: $(\diamondsuit)$
The above corollary provides a first way of computing the inverse A^{-1} of a matrix $A \in \mathrm{mat}_n(R)$. All we have to do is solving the equations $Ax_k = e_k$ for the Euclidean vectors e_k e.g. by the Gaussian algorithm (4.29) or LU-decomposition. For practical computations over a commutative ring R it is best to do this for all n SLEs simultaneously. That is we start with $(A \mid \mathbb{1}_n)$ and regard this as a $(n \times 2n)$-matrix. Then try to bring this into the form $(\mathbb{1}_n \mid B)$ using elementary operations on the rows of $(A \mid B)$. Once we arrived at $(\mathbb{1}_n \mid B)$, we have found the inverse $A^{-1} = B$. The operations allowed, are

1. Interchange two rows of $(A \mid B)$.

2. Multiply one row of $(A \mid B)$ with a common factor $a \in R$.

3. Add or subtract one row of $(A \mid B)$ from another row.

Prob Operations on the rows are multiplications with a matrix S from the left (this will be the topic of the next section). So if we have $(SA \mid S\mathbb{1}_n) = (\mathbb{1}_n \mid B)$ then $B = S\mathbb{1}_n = S$ and hence $BA = SA = \mathbb{1}_n$. And as R is commutative (4.65) implies $AB = \mathbb{1}_n$, too, such that $A^{-1} = B$. By this we also see, that in any step the multiplication of the right-hand matrix and A results in the left-hand matrix.

Note that combining (2) and (3) we can add or subtract a *multiple* of one row from another row. In an integral domain R you may also scratch a common factor a from a row of $(A \mid B)$, as this equals a multiplication by $\frac{1}{a}$ in the quotient field. It would also be possible to use elementary operations of the columns only, but you may not mix both! The algorithm mimics the Gaussian algorithm - let us provide an example of the workings of this method: We compute the inverse of an invertible 4×4 matrix over $\mathbb{Z}$:

$$\begin{array}{rrrr|cccc} 4 & -2 & 5 & 3 & 1 & 0 & 0 & 0 \\ 1 & -1 & 3 & 3 & 0 & 1 & 0 & 0 \\ 0 & -1 & 2 & 1 & 0 & 0 & 1 & 0 \\ -2 & 1 & -2 & 0 & 0 & 0 & 0 & 1 \end{array}$$

First we interchange the first and second row, to move the 1 to the top row. In the next step we eliminate the first column of the left-hand matrix by subtracting 4 times the first row from the second row and adding the double of the first row to the fourth row:

$$\left(\begin{array}{rrrr|rrrr} 1 & -1 & 3 & 3 & 0 & 1 & 0 & 0 \\ 4 & -2 & 5 & 3 & 1 & 0 & 0 & 0 \\ 0 & -1 & 2 & 1 & 0 & 0 & 1 & 0 \\ -2 & 1 & -2 & 0 & 0 & 0 & 0 & 1 \end{array}\right)$$

$$\left(\begin{array}{rrrr|rrrr} 1 & -1 & 3 & 3 & 0 & 1 & 0 & 0 \\ 0 & 2 & -7 & -9 & 1 & -4 & 0 & 0 \\ 0 & -1 & 2 & 1 & 0 & 0 & 1 & 0 \\ 0 & -1 & 4 & 6 & 0 & 2 & 0 & 1 \end{array}\right)$$

We are done with the first row, for now. To iterate we multiply the third row with -1 and interchange the result with the second row. From there we subtract twice the second row from the third row and also add the second row from the fourth row to get one step closer to upper triangular form

$$\left(\begin{array}{rrrr|rrrr} 1 & -1 & 3 & 3 & 0 & 1 & 0 & 0 \\ 0 & 1 & -2 & -1 & 0 & 0 & -1 & 0 \\ 0 & 2 & -7 & -9 & 1 & -4 & 0 & 0 \\ 0 & -1 & 4 & 6 & 0 & 2 & 0 & 1 \end{array}\right)$$

$$\left(\begin{array}{rrrr|rrrr} 1 & -1 & 3 & 3 & 0 & 1 & 0 & 0 \\ 0 & 1 & -2 & -1 & 0 & 0 & -1 & 0 \\ 0 & 0 & -3 & -7 & 1 & -4 & 2 & 0 \\ 0 & 0 & 2 & 5 & 0 & 2 & -1 & 1 \end{array}\right)$$

To eliminate the second-last coefficient in the fourth row we add 2-times the third row to 3-times the forth row. If A wasn't invertible, we might get stuck here, if the last row denies to be continued.

$$\left(\begin{array}{rrrr|rrrr} 1 & -1 & 3 & 3 & 0 & 1 & 0 & 0 \\ 0 & 1 & -2 & -1 & 0 & 0 & -1 & 0 \\ 0 & 0 & -3 & -7 & 1 & -4 & 2 & 0 \\ 0 & 0 & 0 & 1 & 2 & -2 & 1 & 3 \end{array}\right)$$

We're now heading back: Add 7 times row 4 to row 3, add row 4 to row 2 and 3 times row 4 to row 1. This will eliminate the coefficients in the last column up to the lowest one. Doing this, we find

$$\left(\begin{array}{rrrr|rrrr} 1 & -1 & 3 & 0 & -6 & 7 & -3 & -9 \\ 0 & 1 & -2 & 0 & 2 & -2 & 0 & 3 \\ 0 & 0 & -3 & 0 & 15 & -18 & 9 & 21 \\ 0 & 0 & 0 & 1 & 2 & -2 & 1 & 3 \end{array}\right)$$

Here we see, that -3 can be scratched from the third row. From there on, we can add twice row 3 to row 2 and subtract 3-times row 3 from row 1, only leaving the top row. This of course can be handled by adding row 2 to row 1 once more

$$\left(\begin{array}{cccc|cccc} 1 & -1 & 3 & 0 & -6 & 7 & -3 & -9 \\ 0 & 1 & -2 & 0 & 2 & -2 & 0 & 3 \\ 0 & 0 & 1 & 0 & -5 & 6 & -3 & -7 \\ 0 & 0 & 0 & 1 & 2 & -2 & 1 & 3 \end{array}\right)$$

$$\left(\begin{array}{cccc|cccc} 1 & -1 & 0 & 0 & 9 & -11 & 6 & 12 \\ 0 & 1 & 0 & 0 & -8 & 10 & -6 & -11 \\ 0 & 0 & 1 & 0 & -5 & 6 & -3 & -7 \\ 0 & 0 & 0 & 1 & 2 & -2 & 1 & 3 \end{array}\right)$$

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 1 & -1 & 0 & 1 \\ 0 & 1 & 0 & 0 & -8 & 10 & -6 & -11 \\ 0 & 0 & 1 & 0 & -5 & 6 & -3 & -7 \\ 0 & 0 & 0 & 1 & 2 & -2 & 1 & 3 \end{array}\right)$$

Altogether we have found the inverse matrix

$$\begin{pmatrix} 4 & -2 & 5 & 3 \\ 1 & -1 & 3 & 3 \\ 0 & -1 & 2 & 1 \\ -2 & 1 & -2 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -1 & 0 & 1 \\ -8 & 10 & -6 & -11 \\ -5 & 6 & -3 & -7 \\ 2 & -2 & 1 & 3 \end{pmatrix}$$

4.2 Elementary Matrices

In the previous section we have introduced matrices and the computational operations concerning them - namely the matrix multiplication. We will now study different types of special matrices that can be used to build up all the other matrices by virtue of multiplication. This will be of particular interest for solving linear systems of equations, as all these elementary matrices correspond to a single operation on a system of linear equations.

(4.13) Definition:
Let $(R,+,\cdot)$ be any ring and $1 \leq n \in \mathbb{N}$. Then we will define the set $\mathrm{gl}_n(R)$ of **invertible** matrices, the set $\mathrm{tri}_n(R)$ of **upper triangular** matrices and the set $\mathrm{dia}_n(R)$ of **diagonal** matrices to be the following subsets of $\mathrm{mat}_n(R)$. Likewise a matrix $A \in \mathrm{mat}_n(R)$ is said to be a **lower triangular** matrix, iff $A^* \in \mathrm{tri}_n(R)$ is an upper triangular matrix.

$$\begin{aligned}
\mathrm{gl}_n(R) &:= \{\, A \in \mathrm{mat}_n(R) \mid \exists\, B \in \mathrm{mat}_n(R) \;:\; AB = \mathbb{1}_n = BA \,\} \\
\mathrm{tri}_n(R) &:= \left\{\, A \in \mathrm{mat}_n(R) \mid \forall\, 1 \leq j < i \leq n \;:\; \mathrm{ent}_{i,j}(A) = 0 \right\} \\
\mathrm{tri}^1_n(R) &:= \{\, A \in \mathrm{tri}_n(R) \mid \forall\, 1 \leq i \leq n \;:\; \mathrm{ent}_{i,i}(A) = 1 \,\} \\
\mathrm{dia}_n(R) &:= \left\{ \left(\begin{array}{cccc} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & & a_n \end{array} \right) \;\middle|\; a_1, \ldots, a_n \in R \right\}
\end{aligned}$$

(4.14) Proposition: (viz. 1018)
Let $(R,+,\cdot)$ be any ring and $1 \leq n \in \mathbb{N}$. Then the invertible matrices $\mathrm{gl}_n(R)$ are the multiplicative group of the ring mat_R. In particular $\mathrm{gl}_n(R)$ is a (non-commutative) group under the multiplication of matrices

$$\mathrm{gl}_n(R) \;=\; \big(\mathrm{mat}_n(R)\big)^*$$

Also the upper triangular matrices form a sub-ring of the ring $\mathrm{mat}_n(R)$. In particular $\mathrm{tri}_n(R)$ is closed under addition and multiplication of matrices and contains the identity matrix $\mathbb{1}_n$

$$\mathrm{tri}_n(R) \quad \leq_{\mathrm{r}} \quad \mathrm{mat}_n(R)$$

Let now R be a commutative ring and $T = (t_{i,j}) \in \mathrm{tri}_n(R)$ be an upper triangular matrix. Then T is invertible, if and only if for any $i \in 1 \ldots n$ we have $t_{i,i} \in R^*$. And the inverse matrix $T^{-1} \in \mathrm{tri}_n(R)$ is an upper triangular matrix again, such that $\mathrm{tri}_n(R)$ is closed under taking inverses. Also, if T is invertible, we can compute the solution of $Tx = b$ recursively from $i = n$ down to $i = 1$, by

$$\begin{aligned}
x_n &= t_{n,n}^{-1} \\
x_i &= t_{i,i}^{-1} \left(b_i - \sum_{j=i+1}^{n} t_{i,j} x_j \right)
\end{aligned}$$

(4.15) Corollary: (viz. 1019)
If $(R,+,\cdot)$ is a commutative ring and $1 \leq n \in \mathbb{N}$, then any upper triangular matrix $T \in \mathrm{tri}_n^1(R)$ with 1 only on the diagonal is invertible and the inverse T^{-1} is another matrix of this kind. Therefore $\mathrm{tri}_n^1(R)$ is a subgroup of the multiplicative group of $\mathrm{mat}_n(R)$, in formal terms

$$\mathrm{tri}_n^1(R) \quad \leq_{\mathrm{g}} \quad \mathrm{gl}_n(R)$$

Now consider some $A = (a_{i,j})$, $B = (b_{i,j}) \in \mathrm{tri}_n^1(R)$ and suppose that for some $r \in \mathbb{N}$ with $1 \leq r < n$ and any $i \neq j \in 1 \ldots n$ we have both of the implications

(1) If $j \leq r$ then $a_{i,j} = 0$. That is the left r columns of A are 0 apart from the 1 on the diagonal.

(2) If $j > r$ then $b_{i,j} > 0$. That is the right $n - r$ columns of B are 0 apart from the 1 on the diagonal.

$$A = \begin{pmatrix} 1 & & & a_{1,r+1} & \cdots & a_{1,n} \\ & \ddots & & \vdots & & \vdots \\ & & 1 & a_{r,r+1} & & \vdots \\ & & & 1 & \ddots & \vdots \\ & & & & \ddots & a_{n-1,n} \\ & & & & & 1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 1 & b_{1,2} & \cdots & b_{1,r} & & \\ & 1 & \ddots & \vdots & & \\ & & \ddots & b_{r-1,r} & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix}$$

Then the product matrix AB is just composed of A on the left and B on the right (in the form that is shown below). Beware however, that this need not be true for the reverse BA!

$$AB = \begin{pmatrix} 1 & b_{1,2} & \cdots & b_{1,r} & a_{1,r+1} & \cdots & a_{1,n} \\ & \ddots & \ddots & \vdots & \vdots & & \vdots \\ & & \ddots & b_{r-1,r} & \vdots & & \vdots \\ & & & 1 & a_{r,r+1} & & \vdots \\ & & & & 1 & \ddots & \vdots \\ & & & & & \ddots & a_{n-1,n} \\ & & & & & & 1 \end{pmatrix}$$

(4.16) Definition:
Let $(R,+,\cdot)$ be any ring and $1 \leq n \in \mathbb{N}$. Then we will introduce a number of special $(n \times n)$-matrices. First of all, in analogy to the Euclidean bases, for any $r, s \in 1 \ldots n$ we introduce the **Euclidean matrices**

$$E_{r,s} \quad := \quad (\delta_{i,r}\,\delta_{j,s}) \quad \in \quad \mathrm{mat}_n(R)$$

And if $a_1, \ldots, a_n \in R$ are any scalars we can introduce the **diagonal matrix** having the entries a_i to be

$$\mathrm{dia}(a_1, \ldots, a_n) \quad := \quad \sum_{i=1}^{n} a_i\, E_{i,i} \quad = \quad \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & & a_n \end{pmatrix}$$

Another important matrix will simply be denoted by N_n, it is an upper triangular matrix whose only non-zero entries are 1s, one step above (= right of) the diagonal

$$N_n \;:=\; (\delta_{i+1,j}) \;=\; \begin{pmatrix} 0 & 1 & & \\ & 0 & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{pmatrix} \;\in\; \mathrm{tri}_n(R)$$

Now, if $a \in R$ and $i, j \in 1 \ldots n$, we define a **dilatation matrix** $D_i(a)$ and a **translocation matrix** $T_{i,j}(a)$ to be $(n \times n)$-matrices of the following form

$$\begin{aligned} T_{i,j}(a) &:= \mathbb{1}_n + aE_{i,j} \\ D_i(a) &:= \mathbb{1}_n + (a-1)E_{i,i} \end{aligned}$$

Consider any $i, j \in 1 \ldots n$ again, then we define a **transposition matrix** $P_{i,j}$ to to be an $(n \times n)$-matrices of the following form

$$P_{i,j} \;=\; \mathbb{1}_n - E_{i,i} - E_{k,k} + E_{i,k} + E_{k,i}$$

More generally, let us denote the Euclidean basis of R^n by $e_j = (\delta_{i,j})$ again. That is $e_1 = (1,0,0,\ldots,0)$, $e_2 = (0,1,0,\ldots,0)$ and so on until $e_n = (0,\ldots,0,0,1)$. Then for any function $\sigma : 1 \ldots n \to 1 \ldots n$ we define **permutation matrix** P_σ of σ to be the following

$$P_\sigma \;:=\; (\delta_{\sigma(i),j}) \;=\; \begin{pmatrix} \text{—} & e_{\sigma(1)} & \text{—} \\ & \vdots & \\ \text{—} & e_{\sigma(n)} & \text{—} \end{pmatrix} \;\in\; \mathrm{mat}_n(R)$$

We denote the set of all transposition matrices $P_{i,j}$ and all translocation matrices $T_{i,j}(a)$ (where $i, j \in 1 \ldots n$ with $i \neq j$ and $a \in R$) of size n over R by

$$\mathrm{Elm}_n^1(R) \;:=\; \{\, P_{i,j} \mid i,j \in 1 \ldots n \,\} \cup \{\, T_{i,j}(a) \mid i \neq j \in 1 \ldots n,\, a \in R \,\}$$

The set of **elementary matrices** finally consists of all dilatation matrices $D_i(a)$ (where $i \in 1 \ldots n$), all translocation matrices $T_{i,j}(a)$ and all transposition matrices $P_{i,j}$ (where $i \neq j$ again). We denote it by

$$\mathrm{Elm}_n(R) \;:=\; \mathrm{Elm}_n^1(R) \cup \{\, D_i(a) \mid i \in 1 \ldots n,\, a \in R \,\}$$

If finally A and $B \in \mathrm{mat}_{m,n}(R)$ are matrices of the same size over R, then we say that A and B are **elementary equivalent** iff there are elementary matrices $E_1, E_2, \ldots, E_r \in \mathrm{Elm}_m^1(R)$ and $F_1, F_2, \ldots, F_s \in \mathrm{Elm}_n^1(R)$ such that $B = E_1E_2 \ldots E_rAF_1F_2 \ldots F_s$. We denote this by

$$A \equiv B \;:\Longleftrightarrow\; \begin{array}{l} \exists\, E_i \in \mathrm{Elm}_m^1(R) \text{ and } \exists\, F_h \in \mathrm{Elm}_m^1(R) \\ \text{such that } \; B = E_1E_2 \ldots E_rAF_1F_2 \ldots F_s \end{array}$$

(4.17) Remark:
The above definitions are formally correct but some of them are a little bit obfuscated. Hence we wish to enlighten them by rewriting the respective formulas in matrix notation:

- First of all - for $i \neq j$ - the translocation matrix $T_{i,j}(a)$ is just the identity matrix $\mathbb{1}_n$ with the (i,j)-th entry being a instead of 0. Intuitively speaking that is

$$T_{i,j}(a) \;=\; \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & a & & \\ & & & \ddots & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}$$

- By definition the transposition matrix $P_{i,j}$ is the identity matrix in which the (i,i)-th entry 1 is moved to (j,i) and the (j,j)-the entry 1 is moved to (i,j). In that we find that $P_{i,j}$ is the permutation matrix that belongs to $(i\ j)$, i.e. the permutation that interchanges i and j

$$P_{i,j} \;=\; P_{(i\ j)} \;=\; \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 0 & & 1 & & \\ & & & \ddots & & & \\ & & 1 & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}$$

- It is quite obvious that all the matrices of $\mathrm{Elm}_n^1(R)$ are invertible - in fact we will see in (4.21) that $P_{i,j}^{-1} = P_{i,j}$ and $T_{i,j}(a)^{-1} = T_{i,j}(-a)$. Therefore elementary equivalence $\equiv$ is an equivalence relation on the set $\mathrm{mat}_{m,n}(R)$ of matrices of a given size $(m \times n)$.

- Lastly all the dilatation matrices $D_i(a)$ are nothing but a diagonal matrix - start with the identity matrix $\mathbb{1}_n$ but replace the (i,i)-th coefficient by a. That is

$$D_i(a) \;=\; \mathrm{dia}(\ \underbrace{1,\ldots,a,\ldots,1}_{a \text{ at } i\text{-th position}}\) \;=\; \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & a & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}$$

(4.18) Proposition: (viz. 1020)
Let $(R, +, \cdot)$ be any ring and $1 \leq m, n \in \mathbb{N}$. Then we obtain the following formulae when multiplying one of the above matrices with another matrix

(i) For any $r, s \in 1\ldots$ let $E_{r,s} \in \mathrm{mat}_n(R)$ denote the respective Euclidean matrix. Then for any $(m \times n)$-matrix $A \in \mathrm{mat}_{m,n}(R)$ and any $(n \times m)$-matrix $B \in \mathrm{mat}_{n,m}(R)$ we get

$$\begin{aligned} \mathrm{col}_k(AE_{r,s}) &= \begin{cases} \mathrm{col}_r(A) \text{ if } k = s \\ 0 \text{ if } k \neq s \end{cases} \\ \mathrm{row}_i(E_{r,s}B) &= \begin{cases} \mathrm{row}_s(B) \text{ if } i = r \\ 0 \text{ if } i \neq r \end{cases} \end{aligned}$$

(ii) Consider the square matrix $A = (a_{i,j}) \in \mathrm{mat}_n(R)$, then for any four indexes i, j, k and $l \in 1\ldots n$ we have the following identity

$$E_{i,j}\, A\, E_{k,l} = a_{j,k}\, E_{i,l}$$

In particular, if we apply this equation to the identity matrix $A = \mathbb{1}_n = (\delta_{i,j})$, we also get

$$E_{i,j}\, E_{k,l} = \delta_{j,k}\, E_{i,l}$$

(iii) For any $r, s \in 1\ldots$ let $E_{r,s} \in \mathrm{mat}_n(R)$ denote the respective Euclidean matrix again. Also let $a \in R$, $A \in \mathrm{mat}_{m,n}(R)$ and $B \in \mathrm{mat}_{n,m}(R)$. Multiplying with the translocation matrix $T_{r,s}(a)$ from the left adds a-times the s-th row to the r-th row of B. Likewise, multiplying with $T_{r,s}(a)$ from the right adds a-times the r-th column to the s-th column of A. That is for any $i, j \in 1\ldots n$ we get

$$\begin{aligned} \mathrm{col}_k(AT_{r,s}(a)) &= \begin{cases} \mathrm{col}_k(A) + \mathrm{col}_r(A)\, a \text{ if } k = s \\ \mathrm{col}_k(A) \text{ if } k \neq s \end{cases} \\ \mathrm{row}_i(T_{r,s}(a)B) &= \begin{cases} \mathrm{row}_i(B) + a\, \mathrm{row}_s(B) \text{ if } i = r \\ \mathrm{row}_i(B) \text{ if } i \neq r \end{cases} \end{aligned}$$

(iv) Consider any $a_1, \ldots, a_n \in R$ and any $x_1, \ldots, x_n \in R^m$, then the multiplication the diagonal matrix of the a_j is nothing but the scalar multiplication with these elements, formally

$$\mathrm{dia}(a_1, \ldots, a_n) \begin{pmatrix} — & x_1 & — \\ & \vdots & \\ — & x_n & — \end{pmatrix} = \begin{pmatrix} — & a_1x_1 & — \\ & \vdots & \\ — & a_nx_n & — \end{pmatrix}$$

$$\begin{pmatrix} | & & | \\ x_1 & \cdots & x_n \\ | & & | \end{pmatrix} \mathrm{dia}(a_1, \ldots, a_n) = \begin{pmatrix} | & & | \\ x_1a_1 & \cdots & x_na_n \\ | & & | \end{pmatrix}$$

(v) Multiplying N_n from the right shifts the rows up one step, multiplying with N_n from the left shifts the columns right one step. Formally put: Consider any $x_1, \ldots, x_n \in R^m$ then we get

$$N_n \begin{pmatrix} \text{---} & x_1 & \text{---} \\ \text{---} & x_2 & \text{---} \\ & \vdots & \\ \text{---} & x_n & \text{---} \end{pmatrix} = \begin{pmatrix} \text{---} & x_2 & \text{---} \\ & \vdots & \\ \text{---} & x_n & \text{---} \\ \text{---} & 0 & \text{---} \end{pmatrix}$$

$$\begin{pmatrix} | & | & & | \\ x_1 & x_2 & \cdots & x_n \\ | & | & & | \end{pmatrix} N_n = \begin{pmatrix} | & | & & | \\ 0 & x_1 & \cdots & x_{n-1} \\ | & | & & | \end{pmatrix}$$

(vi) If $x_1, \ldots, x_n \in R^m$ again and $\sigma : 1 \ldots n \to 1 \ldots n$ is an arbitrary function, then multiplying with the permutation matrix P_σ from the left permutes the rows with σ, formally

$$P_\sigma \begin{pmatrix} \text{---} & x_1 & \text{---} \\ & \vdots & \\ \text{---} & x_n & \text{---} \end{pmatrix} = \begin{pmatrix} \text{---} & x_{\sigma(1)} & \text{---} \\ & \vdots & \\ \text{---} & x_{\sigma(n)} & \text{---} \end{pmatrix}$$

Now suppose, that $\sigma : 1 \ldots n \to 1 \ldots n$ even is bijective. Then multiplying with the permutation matrix P_σ from the right permutes the columns with σ^{-1}, formally

$$\begin{pmatrix} | & & | \\ x_1 & \cdots & x_n \\ | & & | \end{pmatrix} P_\sigma = \begin{pmatrix} | & & | \\ x_{\sigma^{-1}(1)} & \cdots & x_{\sigma^{-1}(m)} \\ | & & | \end{pmatrix}$$

(4.19) Remark:
In the next section we will introduce the Gaussian algorithm that builds up a matrix $S \in \mathrm{mat}_m(R)$ such that SA is in echelon-form (something like an upper triangular matrix). Let r_i be the i-th row of A

$$A = \begin{pmatrix} \text{---} & r_1 & \text{---} \\ & \vdots & \\ \text{---} & r_m & \text{---} \end{pmatrix} \in \mathrm{mat}_{m,n}(R)$$

As thereby S will be a product $S = E_1 E_2 \ldots E_\ell$ of elementary matrices $E_k \in \mathrm{Elm}_m(R)$ this means that SA is formed out of $A \in \mathrm{mat}_{m,n}(R)$ *by operations on the rows* of A, as we have just seen:

$P_{i,j}\, A$	interchanges r_i and r_j
$T_{i,j}(a)\, A$	adds a-times r_j to r_i
$D_i(a)\, A$	multiplies r_i by a

(4.20) Proposition: (viz. 1018)
Let $(R,+,\cdot)$ be a commutative ring, $1 \leq p, m, n \in \mathbb{N}$ and consider a set of vectors $\{ x_1, x_2, \ldots, x_m \} \subseteq R^p$. Now suppose $\{ y_1, y_2, \ldots, y_n \} \subseteq R^p$ is another set of vectors, that are linear combinations of the x_j

$$y_k \;=\; \sum_{j=1}^{m} a_{j,k} x_j \;\in\; R^p$$

for any $k \in 1 \ldots n$ and some coefficients $a_{j,k} \in R$. Then, if we denote the matrix of these coefficients by $A = (a_{j,k}) \in \mathrm{mat}_{m,n}(R)$, then we find the identity

$$\begin{pmatrix} | & & | \\ y_1 & \cdots & y_n \\ | & & | \end{pmatrix} \;=\; \begin{pmatrix} | & & | \\ x_1 & \cdots & x_m \\ | & & | \end{pmatrix} A$$

(4.21) Corollary: (viz. 1023)
Let $(R,+,\cdot)$ be any ring and $1 \leq n \in \mathbb{N}$, then we summarize our results concerning the inverse matrices of the various elementary matrices

(i) The set of diagonal matrices is a R-subalgebra of $\mathrm{mat}_n(R)$, that is isomorphic to the R-algebra R^n. The isomorphism thereby is given by

$$R^n \;\xrightarrow{\sim}\; \mathrm{dia}_n(R) \;:\; (a_1, \ldots, a_n) \mapsto \mathrm{dia}(a_1, \ldots, a_n)$$

In particular the matrix $\mathrm{dia}(a_1, \ldots, a_n)$ is invertible if and only if all the a_i are invertible in R, i.e. $a_i \in R^*$. And in this case the inverse matrix is given to be

$$\mathrm{dia}(a_1, \ldots, a_n)^{-1} \;=\; \mathrm{dia}(a_1^{-1}, \ldots, a_n^{-1})$$

(ii) In particular the dilatation matrix $D_i(ab)$ is the product of $D_i(a)$ and $D_i(b)$. Therefore $D_i(a)$ is invertible if and only if $a \in R^*$ is a unit in R and in this case the inverse is $D_i(a^{-1})$. Altogether for any $i \in 1 \ldots n$ and any $a, b \in R$ we have the identities

$$\begin{aligned} D_i(a)\, D_i(b) &= D_i(ab) \\ D_i(a)^{-1} &= D_i\left(a^{-1}\right) \end{aligned}$$

(iii) For any $i \neq j \in 1 \ldots n$ the product of the transposition matrices $T_{i,j}(a)$ and $T_{i,j}(b)$ is the transposition matrix $T_{i,j}(a+b)$. In particular any transposition matrix is invertible, the inverse of $T_{i,j}(a)$ For any $i \neq j \in 1 \ldots n$ being $T_{i,j}(-a)$. Altogether for any $i \neq j$ and any $a, b \in R$ we have

$$\begin{aligned} T_{i,j}(a)\, T_{i,j}(b) &= T_{i,j}(a+b) \\ T_{i,j}(a)^{-1} &= T_{i,j}(-a) \end{aligned}$$

(iv) Let us denote the identity map by $id : 1 \dots n \to 1 \dots n : i \mapsto i$. Then clearly the permutation matrix of id is the identity matrix $P_{id} = \mathbb{1}_n$. And if σ and $\tau : 1 \dots n \to 1 \dots n$ are any two functions (not necessarily permutations) on $1 \dots n$, then the product $P_\sigma P_\sigma$ of the permutation matrices is the permutation matrix of $\tau\sigma$ (i.e. in reverse order!), formally

$$P_\sigma P_\tau \;=\; P_{\tau\sigma}$$

In particular the permutation matrix P_σ of σ is invertible, if and only if σ is bijective, and in this case the inverse is the permutation matrix of σ^{-1} which is the transpose of P_σ, altogether

$$P_\sigma^{-1} \;=\; P_{\sigma^{-1}} \;=\; P_\sigma^*$$

(v) If $A = (a_{i,j}) \in \mathrm{mat}_{m,n}(R)$ is any matrix of any size and $\varrho \in S_m$ and $\sigma \in S_n$ are permutations of $1 \dots m$ and $1 \dots n$ respectively, then $P_\varrho A P_\sigma^{-1} \in \mathrm{mat}_{m,n}(R)$ is given to be the matrix

$$P_\varrho \, A \, P_\sigma^{-1} \;= \left(a_{\varrho(i),\sigma(j)}\right) \;= \begin{pmatrix} a_{\varrho(1),\sigma(1)} & \cdots & a_{\varrho(1),\sigma(n)} \\ \vdots & & \vdots \\ a_{\varrho(m),\sigma(1)} & \cdots & a_{\varrho(m),\sigma(n)} \end{pmatrix}$$

4.3 Linear Equations

A **system of equations** is a (finite) collection of equations for several variables $x_1, \dots, x_n$ over some ring R. That is we are given some functions $f_i : R^n \to R$ and some $b_i \in R$ (where $i \in 1 \dots m$) and consider

$$\begin{aligned} f_1(x_1, \dots, x_n) &= b_1 \\ f_2(x_1, \dots, x_n) &= b_2 \\ \vdots \quad \vdots &\quad \vdots \\ f_m(x_1, \dots, x_n) &= b_m \end{aligned}$$

A **solution** of this system of equations is an n-tuple $(x_1, \dots, x_n) \in R^n$ that satisfies all the equations above. The set of solutions is sometimes denoted by

$$\mathbb{L} \;=\; \{\, x \in R^n \mid \forall\, i \in 1 \dots m : f_i(x) = b_i \,\}$$

However the question remains how to solve such a system of equations. In this generality the problem is absolutely unsolvable. In fact very little can be said for sure: In the case $R = \mathbb{R}$ or $R = \mathbb{C}$ there is the *local inversion theorem* which (under certain conditions) guarantees the existence of a solution. The set of solutions is then called a *manifold* and the branch of *differential geometry* studies these. And if all the f_i are polynomial and R is an algebraically closed field, then *algebraic geometry* studies the structure of the set of solutions. To truly find a solution is a different story, however.

The one and only case in which a complete theory of solving a system of equations exists is the case of linear equations. Thereby the system is said to be **linear**, iff all the f_i are multi-linear, i.e. iff any $x_k \mapsto f_i(\dots, x_k, \dots)$ is R-linear. In this case the system of equations is of the form

$$\begin{array}{ccccccccc} a_{1,1}x_1 & + & a_{1,2}x_2 & + & \dots & + & a_{1,n}x_n & = & b_1 \\ a_{2,1}x_1 & + & a_{2,2}x_2 & + & \dots & + & a_{2,n}x_n & = & b_2 \\ \vdots & & & & & & \vdots & = & \vdots \\ a_{m,1}x_1 & + & a_{m,2}x_2 & + & \dots & + & a_{m,n}x_n & = & b_m \end{array}$$

for some fixed *coefficients* $a_{i,k} \in R$ and $b_i \in R$ (where $i \in 1 \dots m$ and $k \in 1 \dots n$). Note that matrices provide a very compact notation for linear systems of equations. Just let $A = (a_{i,k}) \in \mathrm{mat}_n(R)$ be the matrix of the coefficients and $b = (b_1, \dots, b_m) \in R^m$, then the above system boils down to a single equation for vectors (that is finite tuples over R)

$$Ax \;=\; b$$

Still a notation does not provide an algorithm of solving the equations. Now this is the purpose of this section and we start by giving an example:

$$\begin{aligned} (1) \quad 2x_1 + 2x_2 - 3x_3 + 2x_4 &= 8 \\ (2) \quad 2x_1 + 4x_2 + 8x_3 - 4x_4 &= 6 \\ (3) \quad -3x_1 - 4x_2 + x_4 &= 1 \end{aligned}$$

This is a (3×4)-system and we seek all 4-tuples (x_1, x_2, x_3, x_4) satisfying all 3 equations above. The problem is that these equations are interlocked with each other, so let us try to disentangle these equations. We see that subtracting equation (1) from equation (2) the coefficient of x_1 vanishes, so let's try $(2) - (1) \to (2)$. With equation (3) the case is not so simple, but it works out fine with $3(1) + 2(3) \to (3)$

$$\begin{array}{lrcl} (1) & 2x_1 + 2x_2 - 3x_3 + 2x_4 & = & 8 \\ (2) & 2x_2 + 11x_3 - 6x_4 & = & -2 \\ (3) & -2x_2 - 9x_3 + 8x_4 & = & 26 \end{array}$$

So we have reduced the problem by the variable x_1 at the cost of equation (1) - if we continue using (1), then x_1 will reappear. So we restrict ourselves to (2) and (3). To eliminate x_2 let us add (2) and (3) and make the result or equation (3), i.e. $(2) + (3) \to (3)$

$$\begin{array}{lrcl} (1) & 2x_1 + 2x_2 - 3x_3 + 2x_4 & = & 8 \\ (2) & 2x_2 + 11x_3 - 6x_4 & = & -2 \\ (3) & 2x_3 + 2x_4 & = & 24 \end{array}$$

Let us suppose $R = \mathbb{Q}$, then dividing by 2 we found $x_3 + x_4 = 12$ - this is a multitude of solutions, every x_4 gives rise to another x_3 since equation (3) is just $x_3 = 12 - x_4$. But by equation (2) this now means $2x_2 = -2 - 11(12 - x_4) + 6x_4 = -134 + 17x_4$ and hence $x_2 = -67 + 17x_4/2$. This can be inserted into equation (1) $2x_1 = 8 - (-134 + 17x_4) + 3(12 - x_4) + 2x_4 = 178 - 22x_4$ and hence $x_1 = 89 - 11x_4$. Altogether any solution x of this system of equations is of the form

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \in \begin{pmatrix} 89 \\ -67 \\ 12 \\ 0 \end{pmatrix} + \mathbb{Q} \begin{pmatrix} -11 \\ 17/2 \\ -1 \\ 1 \end{pmatrix}$$

(4.22) Example:
Before we proceed to develop a complete theory for solving systems of linear equations (SLE) let us regard some standard examples of vector-geometry. The idea how to solve an SLE always is to add multiples of one equation to another with the aim of finding a new equation in which one variable has been eliminated. In consequence, if there are less equations than variables, there will remain some free variables. These constitute a space of solutions.

- Let us regard the equation $2x_1 + x_2 = 1$ where the variables run over $x = (x_1, x_2) \in \mathbb{R}^2$. This is equivalent, to $x_2 = -2x_1 + 1$ such that we can already write down the general solution of this equation

 $$x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ 1 - 2x_1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} + x_1 \begin{pmatrix} 1 \\ -2 \end{pmatrix}$$

 Geometrically speaking, the set of solutions forms a line in the plane $\mathbb{R}^2$ that runs through $(0, 1)$ in the direction of $(1, -2)$ - refer to section 4.8 for details.

- If we regard the equation $2x_1 + x_2 = 1$ with variables $x = (x_1, x_2, x_3) \in \mathbb{R}^3$ then x_3 clearly is missing. Nevertheless we may rewrite it in the form $x_2 = 1 - 2x_1$. So if we now look at the set of solutions, we find

$$x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1 \\ 1 - 2x_1 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + x_1 \begin{pmatrix} 1 \\ -2 \\ 0 \end{pmatrix} + x_3 \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

 Geometrically speaking, the set of solutions now forms a plane in three dimensional $\mathbb{R}^3$ space that runs through $(0,1,0)$ in the directions of $(1,-2,0)$ and $(0,0,1)$ - this will be covered in 4.8, too.

- The equation $2x_1 - x_2 + 3x_3 = 2$ describes a plane in three dimensional space, that lies perpendicular to $(2,-1,3)$. It is easy to see, that e.g. $(1,0,0)$ is a point contained in that plane. Given another plane, described by $-4 + 4x_2 - 5x_3 = 4$ it stands to reason that the intersection of these two planes should be a line. This line consists of all those $x = (x_1, x_2, x_3) \in \mathbb{R}^3$, that solve both equations *simultaneously*. That is it consists precisely of the solutions of the SLE

$$\begin{array}{rrcl} (1) & 2x_1 - x_2 + 3x_3 & = & 2 \\ (2) & -4x_1 + 4x_2 - 5x_3 & = & 4 \end{array}$$

 It is clear, that we can eliminate x_1 form the second equation, by adding the double of equation (1), that is we replace $2(1) + (2) \to (2)$ and end up, with

$$\begin{array}{rrcl} (1) & 2x_1 - x_2 + 3x_3 & = & 2 \\ (2) & 2x_2 + x_3 & = & 8 \end{array}$$

 This new equation (2) can now be reformulated as $x_3 = 8 - 2x_2$ and if we insert this information into equation (1) we get $2x_1 = 2 + x_2 - 3x_3 = 2 + x_2 - 3(8 - 2x_2) = -22 + 7x_2$. By dividing with 2 (in case of the base ring $R = \mathbb{R}$ this is not a problem) we find $x_1 = -11 + 3.5x_2$. Hence the intersection of the planes is given to be

$$x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} -11 + 3.5x_2 \\ x_2 \\ 8 - 2x_2 \end{pmatrix} = \begin{pmatrix} -11 \\ 0 \\ 8 \end{pmatrix} + x_2 \begin{pmatrix} 3.5 \\ 1 \\ -2 \end{pmatrix}$$

 Geometrically speaking, the set of solutions forms a line in three dimensional space that runs through $(-11,0,8)$ in the direction of $(3.5,1,-2)$. Of course a line was expected, as we started with intersecting two planes.

- Let us now regard two lines in three dimensional space: g runs through $(7,8,0)$ in the direction of $(2,2,-1)$ and h through $(-3,0,9)$ in the direction of $(2,1,3)$

$$g(s) = \begin{pmatrix} 7 \\ 8 \\ 0 \end{pmatrix} + s \begin{pmatrix} 2 \\ 2 \\ -1 \end{pmatrix} \quad h(t) = \begin{pmatrix} -3 \\ 0 \\ 9 \end{pmatrix} + t \begin{pmatrix} 2 \\ 1 \\ -3 \end{pmatrix}$$

We now want to know, whether these lines intersect and (in case they do) at which point that is. To answer this we regard the equation

$$\begin{pmatrix} 7 \\ 8 \\ 0 \end{pmatrix} + s \begin{pmatrix} 2 \\ 2 \\ -1 \end{pmatrix} = \begin{pmatrix} -3 \\ 0 \\ 9 \end{pmatrix} + t \begin{pmatrix} 2 \\ 1 \\ -3 \end{pmatrix}$$

Written explicitly this is a SLE having 3 equations and 2 the variables s and t. We already present this SLE in standard form:

$$\begin{array}{lrcl} (1) & 2s - 2t & = & -10 \\ (2) & 2s - t & = & -8 \\ (3) & -s + 3t & = & 9 \end{array}$$

We now divide equation (1) by to and add the result to (3), that is $(1)/2 \to (1)$ and $(1) + (3) \to (3)$. We hence get

$$\begin{array}{lrcl} (1) & s - t & = & -5 \\ (2) & 2s - t & = & -8 \\ (3) & 2t & = & 4 \end{array}$$

Dividing equation (3) by 2 as well, we find $t = 2$. And if the insert this result into equation (1) we also find $s = -5 + t = -3$. Note that we have not used equation (2) so far, but it also imposes a condition on (s,t). Let us check the result in equation (2): $2s - t = 2 \cdot (-3) - 2 = -8$ is satisfied. That means, $(s,t) = (-3,2)$ truly is a solution of the SLE and in fact we find the common point on the lines g and h:

$$g(-3) \;=\; h(2) \;=\; \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

(4.23) Proposition: (viz. 845)
Let $(R,+,\cdot)$ be an arbitrary ring, $1 \leq m$, $n \in \mathbb{N}$ and consider any matrix $A \in \mathrm{mat}_{m,n}(R)$ over R. Finally let $x \in R^n$ and $b \in R^m$, then we obtain the following statements

(i) Let us denote $\mathbb{L}(Ax = b) := \{\, x \in R^n \mid Ax = b \,\}$ the set of solutions of the linear system $Ax = b$ of equations. If $b \notin \mathrm{im}(A)$ then there is no solution $\mathbb{L}(Ax = b) = \emptyset$. Conversely if $b \in \mathrm{im}(A)$ then there is some *special solution* $u \in R^n$ with $Au = b$. And for any such u the set of solutions is then given to be

$$\mathbb{L}(Ax = b) \;=\; u + \mathrm{kn}(A)$$

(ii) If $S \in \mathrm{gl}_n(R)$ and $T \in \mathrm{gl}_m(R)$ are any two invertible matrices, let us denote $D := SAT \in \mathrm{mat}_{m,n}(R)$. Thereby the following two statements are equivalent

(a) $Ax \;=\; b$

(b) there is some $z \in R^n$ such that $x = Tz$ and $Dz = Sb$

(iii) If we use notation of (i) and (ii) before, then the set of solutions of $Ax = b$ can be reformulated as

$$\mathbb{L}(Ax = b) \;=\; T\,\mathbb{L}(Dx = Sb)$$

(iv) Let us continue with (iii), if $Sb \notin \mathrm{im}(D)$ then there is no solution $\mathbb{L}(Ax = b) = \emptyset$. Conversely if $Sb \in \mathrm{im}(D)$ then there is some $u \in R^n$ with $Du = Sb$. And the set of solutions is then given to be

$$\mathbb{L}(Ax = b) \;=\; Tu + T\,\mathrm{kn}(D)$$

(4.24) Example: (viz. 845) **Diophantine Equation:**
Consider some Euclidean domain (R, ν) such as $R = \mathbb{Z}$ and pick up some coefficients $a_1, \ldots, a_n \in R$ where we assume the $a_i \neq 0$ to be non-zero. Then we consider the linear equation

$$L(x) \;:=\; a_1x_1 + \cdots + a_nx_n \;=\; b$$

where $b \in R$ again. Thereby the set of solutions is $\mathbb{L} = \{\, x \in R^n \mid L(x) = b \,\}$. In order to present a complete set of solutions for this equation let us proceed one step at a time:

- Let us denote a greatest common divisor of the coefficients by $d \in \gcd\{\, a_1, \ldots, a_n \,\}$. Then the equation $L(x) = b$ admits a solution $x \in R^n$ if and only if d divides b. Formally that is

 $$\mathbb{L} \neq \emptyset \quad\Longleftrightarrow\quad d \mid b$$

 This is due to proposition (2.83.(iii)) which tells us, that $\mathrm{im}(L) = dR$. In fact the enhanced Euclidean algorithm (2.72) provides some $u_1, \ldots, u_n \in R$ such that $a_1u_1 + \cdots + a_nu_n = d$. And thereby we get a special solution $s \in R^n$ of $L(x) = b$ by taking

 $$s \;=\; \left(\frac{b}{d}u_1,\; \ldots,\; \frac{b}{d}u_n\right) \;\in\; \mathbb{L}$$

- In case $n = 1$ the solution is quite simple and uniquely determined: Since $d = a_1$ we have a solution to $a_1x_1 = b$ if and only if $a_1 \mid b$. In this case the solution $x_1 = b/a_1$ is uniquely determined and can be computed by division with remainder.

- In case $n \geq 2$ it is clear that the solution cannot be uniquely determined any longer, as L will have a non-zero kernel. In fact we know by (4.23) that $\mathbb{L} = s + \mathrm{kn}(L)$, where s is any solution $L(s) = b$, e.g. the one presented above, using the enhanced Euclidean algorithm. In the next step we will look at the kernel in case $n = 2$ only: Here we find that $\mathrm{kn}(L) = (a_2/d, -a_1/d)R$ such that altogether the set of solutions is given to be

 $$\mathbb{L} \;=\; \left(\frac{b}{d}u_1,\; \frac{b}{d}u_2\right) + \left\{\, \left(\frac{a_2}{d}t,\; -\frac{a_1}{d}t\right) \mid t \in R \,\right\}$$

- In case $n \geq 3$ let us denote some greatest common divisor of the first $k \in 2 \ldots n$ coefficients by $d_k \in \gcd\{\, a_1, \ldots, a_k \,\}$. In the notation above that is $d_n = d$. Also pick up some $u_{i,k} \in R$ (where

$1 \leq i \leq k$, e.g. using the enhanced Euclidean algorithm) such that we get

$$a_1 u_{1,k} + \cdots + a_k u_{k,k} \;=\; d_k$$

We already know $\mathbb{L} = s + \mathrm{kn}(L)$, but we now give an explicit description of the kernel $\mathrm{kn}(L)$ to be the image of the following $n \times (n-1)$ matrix A. That is we have $\mathrm{kn}(L) = \mathrm{im}(A)$ and hence $\mathbb{L} = s + \mathrm{im}(A)$, where

$$A \;=\; \begin{pmatrix} a_2/d_2 & a_3 u_{1,2}/d_3 & \cdots & a_n u_{1,n-1}/d_n \\ -a_1/d_2 & a_3 u_{2,2}/d_3 & \cdots & a_n u_{2,n-1}/d_n \\ 0 & -d_2/d_3 & & a_n u_{3,n-1}/d_n \\ \vdots & 0 & \ddots & \vdots \\ \vdots & \vdots & & a_n u_{n-1,n-1}/d_n \\ 0 & 0 & & -d_{n-1}/d_n \end{pmatrix}$$

Formally that is $A = (a_{i,k}) \in \mathrm{mat}_{n,n-1}(R)$ is the matrix given by the coefficients $(a_{1,1}, \ldots, a_{n,1}) = (a_2/d_2, -a_1/d_2, 0, \ldots, 0)$ and for any $i \in 2 \ldots n$ and $k \in 1 \ldots n-1$ we have

$$a_{i,k} \;:=\; \begin{cases} a_{k+1} u_{i,k}/d_{k+1} \text{ if } i < k \\ -d_k/d_{k+1} \text{ if } i = k \\ 0 \text{ if } i > k \end{cases}$$

Proposition (4.23) provides a strategy for solving linear systems $Ax = b$ of equations: Find invertible matrices S and T such that $D = SAT$ becomes an *easy* matrix. Well, D is *easy* if the equation $Dx = Sb$ can be solved easily. This of course is the case, if D is something like a diagonal matrix - one entry per column - as in this case we do not have an interlocked *system* of equations, but simply n separate equations of the form $a_i x_i = b_i$.
So we will have to define, when the matrix D is *easy* (this will be called the *Gauss-form*) and we have to provide a way of finding S and T - this will be the *Gauss-algorithm*. Then we only have to solve $Du = Sb$ (supposed such an u exists), as then $\mathbb{L}(Ax = b) = Tu + T\,\mathrm{kn}(D)$.

(4.25) Definition:
Let $(R, +, \cdot)$ be an arbitrary ring and $1 \leq m, n \in \mathbb{N}$, then for any n-tuple $a = (a_1, \ldots, a_n) \in R^n$ with $a \neq 0$ we denote the index of the first non-zero entry of a by $\mu(a)$, that is

$$\mu(a) \;:=\; \min\{\, k \in 1 \ldots n \mid a_k \neq 0 \,\} \;\in\; 1 \ldots n$$

Specifically for $a = 0$ we let $\mu(a) := \infty$. Analogously for an $(m \times n)$-matrix $A \in \mathrm{mat}_{m,n}(R)$ with $A = (a_{i,k})$ we let $\mu(0) := \infty$ and for $A \neq 0$ we define $\mu(A)$ to be the index of the first non-zero entry of any of its rows, formally again

$$\begin{aligned} \mu(A) \;&:=\; \min\{\, \mu(\mathrm{row}_i A) \mid i \in 1 \ldots m : a_k \neq 0 \,\} \\ &=\; \min\{\, k \in 1 \ldots n \mid \exists\, i \in 1 \ldots m : a_{i,k} \neq 0 \,\} \end{aligned}$$

(4.26) Definition:
Let $(R,+,\cdot)$ be an arbitrary ring and $1 \leq m,n \in \mathbb{N}$ again, then a matrix $A \in \mathrm{mat}_{m,n}(R)$ is said to be in **echelon-form**, iff either $A = 0$ is zero, or $A \neq 0$ and there is some $r \in 1 \ldots m$ such that:

(1) $\mu(\mathrm{row}_1 A) < \cdots < \mu(\mathrm{row}_r A)$ and

(2) $\forall\, i \in \mathbb{N}$ with $r < i \leq m$ we have $\mathrm{row}_i(A) = 0$

That is the non-zero entries of A form a descending (from top left to bottom right) stair. In particular the zero-rows of A are at the bottom of A. Now A is said to be in **Gauss-form**, iff A is in echelon-form and any non-zero row begins with a $1 \in R$ (not just any non-zero element of R). That is: let $r \in \mathbb{N}$ be as before, $r := \max\{\, i \in 1 \ldots m \mid \mathrm{row}_i A \neq 0 \,\}$ and let us abbreviate $k(i) := \mu(\mathrm{row}_i A)$ for any $i \in 1 \ldots r$, then A is in Gauss-form, iff also

(3) $\forall\, i \in 1 \ldots r$ we get $a_{i,k(i)} = 1$

(4.27) Example:
The following (3×4)-matrix features $r = 2$, $\mu(\mathrm{row}_1 A) = 1$, $\mu(\mathrm{row}_2 A) = 3$ and $\mu(\mathrm{row}_3 A) = \infty$ and hence is in echelon-form. However it is not in Gauss-form, as $\mathrm{ent}_{2,3} A = 2 \neq 1$

$$A \;=\; \begin{pmatrix} 1 & 0 & -1 & 4 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

The next example of a (4×4)-matrix is *not* in echelon-form, as the second column features a double-step. That is $\mu(\mathrm{row}_2 B) = 2$ and $\mu(\mathrm{row}_2 B) = 2$ which contradicts the strict inequality $\mu(\mathrm{row}_2 B) < \mu(\mathrm{row}_2 B)$

$$B \;=\; \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

(4.28) Example:
If a system of linear equations is in Gauss form, then it is truly possible to solve this system. As an example, let us consider the following system

$$\begin{pmatrix} 0 & 1 & 2 & -3 & 1 \\ 0 & 0 & 1 & -4 & 5 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} x \;=\; \begin{pmatrix} -5 \\ 7 \\ 2 \\ 0 \end{pmatrix}$$

Written explicitly - where we denote $x = (x_1, x_2, x_3, x_4, x_5)$ as usual - this system abbreviates the following set of equations

$$\begin{array}{lrcl} (1) & x_2 + 2x_3 - 3x_4 + x_5 & = & -5 \\ (2) & x_3 - 4x_4 + 5x_5 & = & 7 \\ (3) & x_5 & = & 2 \\ (4) & 0 & = & 0 \end{array}$$

First of all it is clear that equation (4) is a void condition, the set $\mathbb{L}$ of solutions is solely determined by equations (1) to (3). This would have been entirely different, if we had the equation $0 = 1$, in this case we had $\mathbb{L} = \emptyset$, as there would be no specific solution u. Also the variable x_1 does not occur in the system at all - due to $\mathrm{col}_1(A) = 0$. Consequently the set $\mathbb{L}$ of solutions will be of the form $R \times L$ for some subset $L \subseteq R^4$.
Let us now turn our attention to solving this system: In this case we already know $x_5 = 2$ and this allows to deduce $x_3 = 7 + 4x_4 - 5x_5 = -3 + 4x_4$ from equation (2). This again can be used in equation (1) to obtain $x_2 = -5 - 2x_3 + 3x_4 - x_5 = -7 - 2(-3 + 4x_4) + 3x_4 = -1 - 5x_4$. Altogether the solutions x are of the form

$$x \;=\; \begin{pmatrix} x_1 \\ -1 - 5x_4 \\ -3 + 4x_4 \\ x_4 \\ 2 \end{pmatrix} \;=\; \begin{pmatrix} 0 \\ -1 \\ -3 \\ 0 \\ 2 \end{pmatrix} + x_1 \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + x_4 \begin{pmatrix} 0 \\ -5 \\ 4 \\ 1 \\ 0 \end{pmatrix}$$

So, as could have been expected from (4.23), the set of solutions $\mathbb{L}$ is of the form $\mathbb{L} = u + K$ where $u = (0, -1, -3, 0, 2)$ is a specific solution to the system and K is the kernel of A, here K is a (rank 2) sub-module of R^5.

(4.29) Lemma: (viz. 848) **Gaussian Algorithm**
Let $(R, +, \cdot)$ be a commutative ring, $1 \leq m$, $n \in \mathbb{N}$ and consider any $(m \times n)$-matrix $A = (a_{i,j}) \in \mathrm{mat}_{m,n}(R)$ over R. There is an $(m \times m)$-matrix $S \in \mathrm{mat}_m(R)$ that is a product of elementary matrices $S = S_1 \dots S_\ell$ where $S_k \in \mathrm{Elm}_m(R)$ such that

$$E \;:=\; S\,A \;\in\; \mathrm{mat}_{m,n}(R)$$

is in echelon-form. By remark (4.19) S thereby encodes operations on the rows of A. And this matrix S can be found using the following **Gaussian-algorithm**, that iterates on the number m of columns of A:

(1) *Initialisation:* Pick up a working matrix $E = (e_{i,j}) := A$ and begin with $S := \mathbb{1}_m$. The algorithm starts with row number $r := 1$.

(2) *Termination:* If the r-th row and all rows below that are zero (that is $\mathrm{row}_i(E) = 0$ for any $i \in r \dots m$), then E is in echelon form and hence we may terminate. Else we commence with step (3).

(3) *Targetting:* Among the r-th to last row of E seek out the row with the first non-zero entry, say this is the s-th row. To be precise we take

$$\begin{aligned} u &:= \min\{\, \mu(\mathrm{row}_v E) \mid v \in r \dots m \,\} \\ s &:= \min\{\, t \in r \dots m \mid \mu(\mathrm{row}_t E) = u \,\} \end{aligned}$$

(4) *The Pivot:* Swap the r-th and the s-th row of E, that is we move the row with the first non-zero entry up to the top row of our current step

$$\begin{aligned} S &:= P_{r,s} S \\ E &:= P_{r,s} E \end{aligned}$$

(5) *The Procedure:* Now, for any $i \in (r+1)\dots m$ proceed as follows: If $e_{i,u} = 0$ then ignore this i, else - if $e_{i,u} \neq 0$ - replace

$$\begin{aligned} S &:= T_{i,r}(-e_{i,u})\, D_i(e_{r,u})\, S \\ E &:= T_{i,r}(-e_{i,u})\, D_i(e_{r,u})\, E \end{aligned}$$

(6) *The Recursion:* Supposed $r < m$ consider the next row, that is replace $r := r+1$ and iterate to step (2). If $m = r$, then terminate the algorithm - E is in echelon-form. Note that step (2) may also terminate the algorithm. In any case we find $E = SA$ a matrix in echelon-form.

(4.30) Remark:

(i) Let us explain the Gaussian algorithm a bit: The main step (5) is where the actual computations are done. If we decode the operations of the elementary matrices they actually become quite simple: In fact for any $i \in (r+1)\dots m$ the algorithm simply multiplies row number i with $e_{r,u}$ and then subtracts $e_{i,u}$ times row number r, that is

$$\mathrm{row}_i E \;:=\; e_{r,u}(\mathrm{row}_i E) - e_{i,u}(\mathrm{row}_r E)$$

(ii) As the algorithm is iterated at most m times and the r-th iteration requires at most $m-r$ row-operations (as described in (i) above) the algorithm needs a total of at most $m(m-1)/2$ row-operations.

(iii) If R is a field, then $\mathrm{Elm}_m(R) \subseteq \mathrm{gl}_m(R)$ all elementary matrices are invertible and hence S is invertible, too, being a product of such matrices.

(iv) If R is a field, the matrix $E = (e_{i,j})$ in echelon form can easily be processed into a matrix G in Gauss-form: Let r be the number of non-zero rows of E, that is $r = \#\{\, i \in 1\dots m \mid \mathrm{row}_i E \neq 0 \,\}$. Further let $k(i) := \mu(\mathrm{row}_i E) \in 1\dots n$ and $e_i := e_{i,k(i)}$ and

$$\begin{aligned} D &:= \mathrm{dia}\left(\frac{1}{q_1}, \dots, \frac{1}{q_r}, 1, \dots, 1\right) \\ G &:= DE \end{aligned}$$

Then G is in Gauss-form, $T = DS$ is a product of elementary matrices still, and $G = TA$. And as we will see in (v) this allows to solve the system of linear equations $Ax = b$.

(v) Suppose we are given a system of linear equations $Ax = b$ over a field R. We then use the Gaussian algorithm and (iv) to find a matrix $T \in \mathrm{gl}_m R$ such that $G = TA$ is in Gauss form. Then by (4.23) the set of solutions of $Ax = b$ is given to be:

$$\mathbb{L}(Ax = b) \;=\; \mathbb{L}(Gx = Tb)$$

Hence it remains to solve the equation $Gx = Tb$. But as $G = (g_{i,j})$ is in Gauss form this is feasible: also refer to the example above.

For a more formal approach let us denote the number of non-zero rows of G by $r \in 0 \dots m$, that is $r := \#\{\, i \in 1 \dots m \mid \mathrm{row}_i G \neq 0 \,\}$. Also let $k(i) := \mu(\mathrm{row}_i G) \in 1 \dots n$ and $g_i := g_{i,k(i)}$ again. Then we we can iteratively compute the solution beginning with $i = r$ down to $i = 1$

$$x_{k(i)} \;=\; [Tb]_i - \sum_{j=k(i)+1}^{n} g_{i,j} x_j$$

Thereby all the variables $\{\, x_1, \dots, x_n \,\} \setminus \left\{\, x_{k(1)}, \dots, x_{k(r)} \,\right\}$ remain undetermined. That is any choice of these variables produces a solution, whereas the variables $x_{k(1)}, \dots, x_{k(r)}$ are determined by these indeterminates. In other words the kernel of G is $(n-r)$-dimensional subspace of R^n and the set of solutions is of the form

$$\mathbb{L}(Ax = b) \;=\; u + \mathrm{kn}(G)$$

(vi) It might be helpful to reformulate the Gaussian algorithm in pseudo-code, so that's what we want to do now: First of all we will need the following variables: $A = (a_{i,j})$ and $E = (e_{i,j}) \in \mathrm{mat}_{n,m} R$, $S = (s_{i,j}) \in \mathrm{mat}_m(R)$ also i, r, s and $u \in \mathbb{N}$ and finally swap $\in R^n$.

```
S ← 𝟙_m
E ← A
r ← 1
while (r < m) and (∃ s ∈ r ... m : row_s(E) ≠ 0) do begin
    u ← min{ μ(row_v(E)) | v ∈ r ... m }
    s ← min{ t ∈ r ... m | μ(row_t(E)) = u }
    if (s ≠ r) then begin
        swap ← row_r(E)
        row_r(E) ← row_s(E)
        row_s(E) ← swap
    end-if
    for i := r + 1 to m step 1 do begin
        row_i(S) ← s_{r,u}(row_i(S)) − s_{i,u}(row_r(S))
        row_i(E) ← e_{r,u}(row_i(E)) − e_{i,u}(row_r(E))
    end-for
    r ← r + 1
end-while
```

(4.31) Example:
We would like to enlighten things a little, by presenting an example of the workings of the Gaussian algorithm in the case of the following example

$$A \;=\; \begin{pmatrix} 0 & 1 & 2 & -3 & 1 \\ 0 & 1 & 4 & -7 & 6 \\ 0 & 2 & 4 & -6 & 2 \\ 0 & -1 & 1 & 3 & 0 \end{pmatrix}$$

First of all the Gauss-algorithm initializes $E := A$, $S := \mathbb{1}_m$ and starts with row $r = 1$ now, as A is non-zero the algorithm does not terminate right away. As the 1-st column of E has a minimal non-zero entry we get $u = 2$ and $s = 1$. Now as $r = s$ there is no need to pivot (we have $e_{2,1} = 1 \neq 0$).

In the central step, for $i = 2$, we get $S = T_{2,1}(-1)\, D_2(1)$ and multiply E with $T_{2,1}(-1)\, D_2(1)$ from the left. That is the 2-nd row is multiplied with 1 (which changes nothing) and then -1 times the 1-st row is added to the 2-nd row. Likewise for $i = 3$ we multiply with $T_{3,1}(-2)\, D_3(1)$ from the left again. That is the 3-rd row is multiplied with 1 (void again) and then -2 times the 1-st row is added to the 3-rd row. Finally for $i = 4$ we multiply with $T_{4,1}(1)\, D_4(1)$ from the left, that is we add the 1-st row to the 4-th row. So far we've got $S = T_{4,1}(1)\, D_4(1)\, T_{3,1}(-2)\, D_3(1)\, T_{2,1}(-1)\, D_2(1)$ and $E = SA$ which amounts to

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ -2 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 & -3 & 2 \\ 0 & 1 & 4 & 8 & -4 \\ 0 & 2 & 4 & 0 & 1 \\ 0 & -1 & -2 & 3 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 & -3 & 2 \\ 0 & 0 & 2 & -4 & 5 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 1 \end{pmatrix}$$

Now the Gauss-algorithm iterates with $r = 2$. The first column with non-zero entries (from row 2 on) is $s = 2$ with $u = 3$, so again there is no need to pivot ($e_{3,2} = 2 \neq 0$). However for $i = 3$ we find $e_{3,2} = 0$ and hence we continue with $i = 4$ already. Hereby we multiply with $T_{4,2}(-3)\, D_4(2)$ from the left which is: First multiply row 4 with 2 and then add -3 times the second row to row 4. So S has risen to $S = T_{4,2}(-3)\, D_4(2)\, T_{4,1}(1)\, T_{3,1}(-2)\, T_{2,1}(-1)$ (omitting identity matrices) and this step yielded the matrices

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -3 & 0 & 2 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 & -3 & 2 \\ 0 & 0 & 2 & -4 & 5 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 & -3 & 2 \\ 0 & 0 & 2 & -4 & 5 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 12 & -13 \end{pmatrix}$$

As we have a zero-row $\mathrm{row}_3 E = 0$ the following step $r = 3$ will be the last one to take. But let's stick to the letter: Here we get $u = 4$ and $s = 4$ so we have to swap rows 3 and 4 by multiplying $P_{3,4}$ from the left. So by now we found the matrices

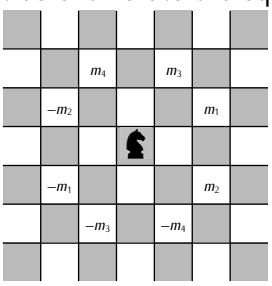
$$S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -3 & 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ -2 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 5 & -3 & 0 & 2 \\ -2 & 0 & 1 & 0 \end{pmatrix}$$

$$E = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 5 & -3 & 0 & 2 \\ -2 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 & -3 & 1 \\ 0 & 1 & 4 & -7 & 6 \\ 0 & 2 & 4 & -6 & 2 \\ 0 & -1 & 1 & 3 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 & -3 & 1 \\ 0 & 0 & 2 & -4 & 5 \\ 0 & 0 & 0 & 12 & -13 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

In step $r = 4$ we see that $\mathrm{row}_4 E = 0$ already, hence the termination condition (2) of the Gaussian algorithm is satisfied. And in fact, we see that E is in echelon-form already.

Note that this does not represent the modified linear system of equations that we computed in the introductory example. The reason is that in the manual computation we have evaded the common multiple of 2 in the first step $(2) - (1) \to (2)$. But the Gauss-algorithm does not check for common multiples.

(4.32) Example:
Here's a complimentary example for those chess-players out there: Let us consider a knight on a chess-board (of infinite size). We want to know, whether it can reach any square and what the redundancies are, when moving this chess piece. So let us enumerate the squares the knight may move to



If it starts at $(0,0)$ the valid movements are $m_1 = (2,1)$, $m_2 = (2,-1)$, $m_3 = (1,2)$ and $m_4 = (-1,2)$. We only need to count the number of times the knight is moved in the directions m_1 to m_4, as the sequel of moves has no impact on the end location. Altogether the possible locations the knight may move to are the image of the following matrix

$$M \;=\; \begin{pmatrix} 2 & 2 & 1 & -1 \\ 1 & -1 & 2 & 2 \end{pmatrix}$$

As $M(-1,1,1,0) = (1,0)$ and $M(0,-1,1,-1) = (0,1)$ we see, that the knight may reach any square on the chess board, given time. So if we want to reach square (x,y) we can use the number n_i of moves in direction m_i given by $(n_1,n_2,n_3,n_4) = (-x, x-y, x+y, -y)$. We will prove shortly that the kernel of M is the following:

$$\mathrm{kn}(M) \;=\; \mathbb{Z}\begin{pmatrix} 1 \\ 1 \\ -2 \\ 2 \end{pmatrix} + \mathbb{Z}\begin{pmatrix} 0 \\ 4 \\ -3 \\ 5 \end{pmatrix}$$

So these are the non-trivial moves, that return the knight to its starting location (e.g. a trivial move would be m_1, m_2, $-m_1$, $-m_2$). Combining all this with (4.23.(i)) we see that the possible numbers $n = (n_1,n_2,n_3,n_4)$ of moves to take the knight to square (x,y) are

$$\mathbb{L}\left(Mn = \begin{pmatrix} x \\ y \end{pmatrix}\right) \;=\; \begin{pmatrix} -x \\ x-y \\ x+y \\ -y \end{pmatrix} + \mathbb{Z}\begin{pmatrix} 1 \\ 1 \\ -2 \\ 2 \end{pmatrix} + \mathbb{Z}\begin{pmatrix} 0 \\ 4 \\ -3 \\ 5 \end{pmatrix}$$

Prob It is easy to verify $(a, a+4b, -2a-3b, 2a+5b) \in \mathrm{kn}(M)$ for any a, $b \in \mathbb{Z}$. Conversely consider $n \in \mathrm{kn}(M)$ and let $a := n_1$. As $n_3 + n_4 = (n_3 - n_4) + 2n_4 = -2(n_1+n_2) + 2n_4$ we have $2 \mid n_3 + n_4$. As also $n_2 - n_1 = 2(n_3+n_4)$ we get $4 \mid n_2 - n_1$. Let $b := (n_2 - n_1)/4$ then $n_2 = a + 4b$. Eliminating n_4 from M we get $5n_1 + 3n_2 + 4n_3 = 0$ and from this $n_3 = -2a - 3b$. Eliminating n_3 from M we get $3n_1 + 5n_2 - 4n_4 = 0$ and hence also $n_4 = 2a + 5b$.

Let us close this section with another algorithm to solve SLEs with an equal number of variables and equations over a field. This is a rather common situation and this algorithm is particularly useful, if you need to solve $Ax = b$ for lots of different b. However it also requires A to be an invertible matrix:

(4.33) Proposition: (viz. 849)
Let $(F, +, \cdot)$ be a field and $A \in \mathrm{gl}_{n+1}(F)$ an invertible, square matrix over F. Then there are matrices P_1 to P_n and L_1 to L_n all in $\mathrm{mat}_{n+1}(F)$ satisfying the following three properties

(1) Any P_k (where $1 \leq k \leq n$) is the permutation matrix of a transposition of the form $(k\, q(k))$, that is $P_k = P_{(k\, q(k))}$, where $k \leq q(k) \leq n+1$. In particular $P_k^2 = \mathbb{1}_{n+1}$.

(2) Any L_k (where $1 \leq k \leq n$) is $\mathbb{1}_{n+1}$ augmented by some entries on the k-th column, below the diagonal. That is $\mathrm{ent}_{i,j}(L_k) = 1$ for $i = j$ and for $i \neq j$ we have: $\mathrm{ent}_{i,j}(L_k) = 0$ whenever $j \neq k$ or $i < k$. In particular $L_k^* \in \mathrm{tri}_n^1(F)$ such that L_k is invertible.

(3) The matrix $U := L_n P_n \ldots L_2 P_2 L_1 P_1 A \in \mathrm{tri}_n(F)$ is an upper triangular matrix.

For any $k \in 1 \ldots n$ let us denote $\widehat{L}_k := P_n \ldots P_{k+1} L_k P_{k+1} \ldots P_n$, then the $\widehat{L}_k$ are of the same shape, as L_k (as described in (2) above). Let us also denote the permutation matrix $P := P_n \ldots P_2 P_1$ and likewise $\widehat{L} := \widehat{L}_n \ldots \widehat{L}_2 \widehat{L}_1$. Then we have $\widehat{L}^* \in \mathrm{tri}_{n+1}^1(F)$ and we can rewrite the equation in (3) in the form

$$U \;=\; \widehat{L}PA \;\in\; \mathrm{tri}_{n+1}(F)$$

(4.34) Remark:

(i) By property (2) above, any L_k is $\mathbb{1}_{n+1}$ up to entries on the k-th column below the diagonal. In the proof we will use the term *lower-k-columns-only* for matrices of this kind. The same is true for $\widehat{L}_k$ as it is just L_k subjected to a permutation of these lower-k-column entries

$$L_k \;=\; \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & \ell_{k+1,k} & 1 & \\ & & \vdots & & \ddots \\ & & \ell_{n+1,k} & & 1 \end{pmatrix}$$

(ii) This allows to compute the solution x of the SLE $Ax = b$: The proposition grants an upper triangular matrix U, a lower triangular matrix L and a permutation matrix P such that $U = LPA$. Therefore we can compute the solution $x \in F^{n+1}$ in the following way:

- compute $y := \widehat{L}Pb$
- solve $Ux = y$ for x, using (4.14)

Prob as both P and $\widehat{L}$ are invertible $Ax = b$ is equivalent to $\widehat{L}PAx = \widehat{L}Pb$ and this is $Ux = y$.

(iii) *LU-decomposition*: As $\widehat{L}$ only has 1 on its diagonal, its determinant is $\det(L) = 1$ and thereby $\widehat{L}^{-1} = \widehat{L}^{\#}$. Clearly $\widehat{L}^{\#}$ is a lower triangular matrix with all 1 on the diagonal, again. And from $U = \widehat{L}PA$ we then get the decomposition of PA

$$PA \;=\; \widehat{L}^{-1}\,U$$

That is we have found an upper triangular matrix $U \in \mathrm{tri}_{n+1}(F)$ and a lower triangular matrix $L := \widehat{L}^{-1}$ such that $L^* \in \mathrm{tri}^1_{n+1}(F)$ and A is decomposed into L and U, up to permutation P.

(iii) Let us present some pseudo-code for how to compute the P_k, L_k and U of proposition (4.33) for a given matrix $A \in \mathrm{gl}_{n+1}(F)$. Note that the choice of $q(k)$ is arbitrary, for computations by hand it might be best to watch out for divisibilities. Considering numeric stability in a computer algebra programs it is advisible to pick the $q(k)$ such that $|[U]_{q(k),k}|$ is maximal.

$U \leftarrow A$
for $(k = 1)$ to n do begin
 choose $q(k) \in k \ldots n+1$ such that $\mathrm{ent}_{q(k),k}(U) \neq 0$
 $L_k \leftarrow \mathbb{1}_{n+1}$
 $P_k \leftarrow P_{(q(k)\,k)}$
 swap $\leftarrow \mathrm{row}_k(U)$
 $\mathrm{row}_k(U) \leftarrow \mathrm{row}_{q(k)}(U)$
 $\mathrm{row}_{q(k)}(U) \leftarrow$ swap
 for $(i = k+1)$ to $(n+1)$ do begin
 $\mathrm{ent}_{i,k}(L_k) \leftarrow -\mathrm{ent}_{i,k}(U) \cdot \mathrm{ent}_{k,k}(U)^{-1}$
 $\mathrm{row}_i(U) \leftarrow \mathrm{row}_i(U) + \mathrm{ent}_{i,k}(L_k) \cdot \mathrm{row}_k(U)$
 end-for
end-for

(iv) The best way to track and compute this algorithm is to use a tableau of the following form: Note that the method, how to get L_k from $P_k U_{k-1}$, is described in the algorithm above

k	τ	U_{k-1}	P_k	$P_k U_{k-1}$	L_k
1	$(1\ q(1))$	$U_0 = A$	$P_{(1\,q(1))}$	$P_1 U_0$	L_1
2	$(2\ q(2))$	$L_1 P_1 U_0$	$P_{(2\,q(2))}$	$P_2 U_1$	L_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
n	$(n\ q(n))$	$L_{n-1} P_{n-1} U_{n-2}$	$P_{(n\,q(n))}$	$P_n U_{n-1}$	L_n
$n+1$		$U = L_n P_n U_{n-1}$			

(v) Recall the (4×4)-matrix that we inverted at the end of section 4.1 and take it for A. If we choose $q(1) = 2$, $q(2) = 3$ and $q(3) = 4$ that is $P_1 = P_{(1\,2)}$, $P_2 = P_{(2\,3)}$ and $P_3 = P_{(3\,4)}$ respectively, then the LU-algorithm above turns A into the form $U = \widehat{L}PA$, which becomes

$$\begin{pmatrix} 1 & -1 & 3 & 3 \\ 0 & -1 & 2 & 1 \\ 0 & 0 & 2 & 5 \\ 0 & 0 & 0 & 0.5 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 2 & -1 & 1 & 0 \\ -1 & 0.5 & 1.5 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 4 & -2 & 5 & 3 \\ 1 & -1 & 3 & 3 \\ 0 & -1 & 2 & 1 \\ -2 & 1 & -2 & 0 \end{pmatrix}$$

4.4 Matrix Representations

As we have seen so far, matrices do provide two things: They can be used to formalize and solve linear systems of equations and they enable us to study explicit examples of linear maps. In short they allow computations in module theory of modules of the form R^n. However a finitely generated, free R-modules always is *isomorphic* to such an R-module. So in this section we address the topic how to pull general module theory (of finitely generated, free R-modules) into the computational range of matrices.
To do this we clearly have to fix an isomorphism $M \xrightarrow{\sim} R^n$ by choosing an R-basis $\mathcal{M} = \{ m_1, \ldots, m_n \}$. But this alone does not suffice: As bases are sets only, we have to decide which element of the basis corresponds to the first coordinate, which to the second and so on. That is we have to fix a certain order on the basis $\mathcal{M}$ - otherwise the isomorphsim $M \xrightarrow{\sim} R^n$ is only determined up to permutations of basis elements. That is, instead of a set $\mathcal{M} = \{ m_1, \ldots, m_n \} \subseteq M$ we have to fix a tuple $\mathcal{M} = (m_1, \ldots, m_n)$. So let us recall the definition of an ordered basis:

(4.35) Definition:
Let $(R, +, \cdot)$ be an arbitrary ring and M be an R-module. Then an n-tuple $\mathcal{M} = (m_1, \ldots, m_n)$ where $1 \leq n \in \mathbb{N}$ and $m_i \in M$ is said to be an **(finite) ordered R-basis** of M, iff it satisfies

(1) $\{ m_1, \ldots, m_n \} \subseteq M$ is an R-basis of M

(2) the m_i are pairwise distinct: $m_i = m_j \implies i = j$

(4.36) Remark:

(i) By definition any R-module M, that has a basis is called *free*, but most modules aren't. Hence an R-module M only has an ordered basis, iff it is both, free and finitely generated.

If R is commutative or a skew-field, then the number n of basis elements is uniquely determined however - refer to (3.100). And this number n has been called the *dimension* of M

$$n \;=\; \dim(M)$$

(ii) The standard basis of R^n itself is the so-called *Euclidean basis* $\mathcal{E}(n) := \{ e_1, \ldots, e_n \}$ where for any $j \in 1 \ldots n$ we chose $e_j = (\delta_{i,j}) \in R^n$. Written explicitly that is

$$\begin{aligned} e_1 &= (1,0,0,\ldots,0,0) \\ e_2 &= (0,1,0,\ldots,0,0) \\ \vdots &\quad\; \vdots \\ e_n &= (0,0,0,\ldots,0,1) \end{aligned}$$

By abuse of notation we denote the *ordered* basis $\mathcal{E}(n) := (e_1, \ldots, e_n)$ composed of these Euclidean vectors, by the same symbol $\mathcal{E}(n)$ or simply by $\mathcal{E}$. This should not cause any problems, however.

(4.37) Definition:
Let $(R,+,\cdot)$ be a ring and M, N be R-modules again. Also fix some ordered basis $\mathcal{M} = (m_1,\ldots,m_s) \subseteq M$ and $\mathcal{N} = (n_1,\ldots,n_r) \subseteq N$ of M and N respectively. If now $x \in M$ then we denote

$$[x]_{\mathcal{M}} \;:=\; (x_1,\ldots,x_s) \;\in\; R^s \quad \text{where} \quad x \;=\; \sum_{j=1}^{s} x_j\, m_j$$

and $[x]_j := x_j \in R$, the j-th coefficient of x with respect to the basis $\mathcal{M}$. Also if $\varphi : M \to N$ is a homomorphism of R-modules, then we define the $(r \times s)$-matrix (where $i \in 1\ldots r$ and $j \in 1\ldots s$)

$$[\varphi]^{\mathcal{N}}_{\mathcal{M}} \;:=\; \Big(\big[\varphi(m_j)\big]_i \Big) \;\in\; \mathrm{mat}_{r,s}(R)$$

(4.38) Remark:

(i) Let us give an alternative definition of the matrix representation of φ: The coefficients $a_{i,j} \in R$ of $[\varphi]^{\mathcal{N}}_{\mathcal{M}} = (a_{i,j})$ are the representations of $\varphi(m_j)$ in terms of the basis $\mathcal{N}$. And thereby the coefficients $a_{i,j}$ are defined by the property

$$\varphi(m_j) \;=\; \sum_{i=1}^{r} a_{i,j}\, n_i$$

That is the j-th column of $[\varphi]^{\mathcal{N}}_{\mathcal{M}}$ is the basis representation of the image of the j-th basis vector of M in terms of the chosen basis of N

$$[\varphi]^{\mathcal{N}}_{\mathcal{M}} \;:=\; \begin{pmatrix} | & & | \\ [\varphi(m_1)]_{\mathcal{N}} & \cdots & [\varphi(m_s)]_{\mathcal{N}} \\ | & & | \end{pmatrix}$$

(ii) In case of an endomorphism $\varphi : M \to M$ where we fix the same ordered basis $\mathcal{M}$ on both the preimage M and image M we just write

$$[\varphi]_{\mathcal{M}} \;:=\; [\varphi]^{\mathcal{M}}_{\mathcal{M}}$$

And if the bases $\mathcal{M}$ of M and $\mathcal{N}$ of N are understood, we will often simplify the notation by omitting the bases names, that is we write $[x]$ instead of $[x]_{\mathcal{M}}$ and $[\varphi]$ instead of $[\varphi]^{\mathcal{N}}_{\mathcal{M}}$.

(iii) In case $M = R^s$ there is no difference between the element $x \in M$ itself and its representation in terms of the ordered Euclidean basis $\mathcal{E}(s)$: Consider $x = (x_1,\ldots,x_s) \in R^s$ then clearly $x = \sum_j x_j e_j$ and thereby x is precisely its representation in this basis

$$x \;=\; [x]_{\mathcal{E}(s)}$$

(4.39) Example:
As an example let us regard the polynomial ring $R[t]$ as an R-module. Clearly $R[t]$ is free, as its basis is given by the monomials $\{ t^k \mid k \in \mathbb{N} \}$. The *derivative* $\partial : R[t] \to R[t]$ is the following map

$$\partial \left(\sum_{k=0}^{\infty} a_k \, t^k \right) \; := \; \sum_{k=1}^{\infty} k a_k \, t^{k-1} \; = \; \sum_{k=0}^{\infty} (k+1) a_{k+1} \, t^k$$

In order to give a matrix representation of the map ∂ we have have to restrict ourselves to a finitely generated sub-module of $R[t]$. That is we fix a number $n \in \mathbb{N}$ and regard the R-module of polynomials of degree up to n.

$$M \; := \; \{ f \in R[t] \mid \deg(f) \leq n \}$$

Note that this no longer is a ring, as it is no longer closed under multiplication. It still is closed under addition and scalar multiplication and hence an R-module. It stands to reason to pick up the following ordered basis of M: $\mathcal{T} := (1, t, t^2, \ldots, t^n)$. Then M is isomorphic to R^{n+1} under the isomorphism

$$R^{n+1} \; \xrightarrow{\sim} \; M \; : \; (a_0, a_1, \ldots, a_n) \mapsto \sum_{k=0}^{n} a_k \, t^k$$

And as $\partial(t^k) = k t^{k-1}$ maps one base element to a multiple of another, the derivative $\partial : M \to M$ has the following matrix representation with respect to this ordered basis $\mathcal{T}$:

$$[\partial] \; = \; \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 2 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 3 & & 0 \\ \vdots & \vdots & \vdots & & \ddots & \\ 0 & 0 & 0 & 0 & \cdots & n-1 \\ 0 & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

(4.40) Lemma: (viz. 1024)
Let $(R, +, \cdot)$ be any ring, M be a finitely generated, free R-module and fix an ordered basis $\mathcal{M} \subseteq M$. Then $x \mapsto [x]_{\mathcal{M}}$ is R-linear, that is for any vectors $x, y \in M$ and some scalar $a \in R$ we get

$$\begin{aligned} [ax]_{\mathcal{M}} &= a \, [x]_{\mathcal{M}} \\ [x+y]_{\mathcal{M}} &= [x]_{\mathcal{M}} + [y]_{\mathcal{M}} \end{aligned}$$

Now consider another finitely generated, free R-module N and fix an ordered basis $\mathcal{N} \subseteq N$ again. Then $\varphi \mapsto [\varphi]_{\mathcal{M}}^{\mathcal{N}}$ is R-linear, as well, that is if φ and $\psi : M \to N$ are homomorphisms of R-modules, then

$$\begin{aligned} [a\varphi]_{\mathcal{M}}^{\mathcal{N}} &= a \, [\varphi]_{\mathcal{M}}^{\mathcal{N}} \\ [\varphi+\psi]_{\mathcal{M}}^{\mathcal{N}} &= [\varphi]_{\mathcal{M}}^{\mathcal{N}} + [\psi]_{\mathcal{M}}^{\mathcal{N}} \end{aligned}$$

Finally let L be a third finitely generated, free R-module and fix another ordered basis $\mathcal{L} \subseteq L$. For the following three equations we also require R to be commutative! If now $\varphi : L \to M$ and $\psi : M \to N$ are homomorphisms of R-modules and $x \in L$, then the composition of maps is compatible with the matrix multiplication, that is we find

$$\begin{aligned} [\varphi(x)]_{\mathcal{M}} &= [\varphi]_{\mathcal{L}}^{\mathcal{M}} [x]_{\mathcal{L}} \\ [\psi\varphi]_{\mathcal{L}}^{\mathcal{N}} &= [\psi]_{\mathcal{M}}^{\mathcal{N}} [\varphi]_{\mathcal{L}}^{\mathcal{M}} \end{aligned}$$

In particular, φ is an isomorphism, if and only if its matrix representation is invertible. In this case the matrix representation of φ^{-1} is precisely the inverse matrix of $[\varphi]_{\mathcal{M}}^{\mathcal{N}}$ formally

$$\left[\varphi^{-1}\right]_{\mathcal{N}}^{\mathcal{M}} = \left([\varphi]_{\mathcal{M}}^{\mathcal{N}}\right)^{-1}$$

Let $\mathcal{M} = (m_1, m_2, \ldots, m_s)$ and $\mathcal{N} = (n_1, n_2, \ldots, n_r)$, then the representation of a module homomorphism φ as a matrix $[\varphi]_{\mathcal{M}}^{\mathcal{N}}$ is an isomorphism in itself, from the R-module $\mathrm{mhom}(M, N)$ to the R-module $\mathrm{mat}_{r,s}(R)$. That is we find the following isomorphy

$$\mathrm{mhom}(M, N) \xrightarrow{\sim} \mathrm{mat}_{r,s}(R) \ : \ \varphi \mapsto [\varphi]_{\mathcal{M}}^{\mathcal{N}}$$

The inverse map can be constructed as follows: Given $A \in \mathrm{mat}_{r,s}(R)$ then we need to define $\varphi_A : M \to N$ such that $[\varphi_A]_{\mathcal{M}}^{\mathcal{N}} = A$. For $x \in M$ we have $[x]_{\mathcal{M}} \in R^s$ and hence $A[x]_{\mathcal{M}} \in R^r$ such that we may take

$$\varphi_A(x) := \sum_{i=1}^{r} [A[x]_{\mathcal{M}}]_i \, n_i$$

(4.41) Remark:
Let L and M be R-modules and fix the ordered bases $\mathcal{L} = (\ell_1, \ldots, \ell_t)$ and $\mathcal{M} = (m_1, \ldots, m_s)$ respectively. Let also $\varphi : L \to M$ be an R-module-homomorphism and denote its matrix representation concerning these bases by $A = [\varphi] \in \mathrm{mat}_{s,t}(R)$. If now $x \in L$ is a vector, then the property $[\varphi(x)] = [\varphi][x]$ is just the commutativity of the following diagram:

$$\begin{array}{ccccc} & x & \longmapsto & \varphi(x) & \\ x & L & \longrightarrow & M & y \\ \downarrow & \updownarrow & \circlearrowleft & \updownarrow & \downarrow \\ [x] & R^t & \longrightarrow & R^s & [y] \\ & u & \longmapsto & Au & \end{array}$$

And if N is another R-module with the ordered R-basis $\mathcal{N} = (n_1, \ldots, n_r)$ and $\psi : M \to N$ is another homomorphism of R-modules having the matrix representation $B = [\psi] \in \mathrm{mat}_{r,s}(R)$, then the property $[\psi\varphi] = [\psi][\varphi]$ is just another commutative diagram:

$$\begin{array}{ccccc} L & \xrightarrow{\varphi} & M & \xrightarrow{\psi} & N \\ \updownarrow & \circlearrowleft & \updownarrow & \circlearrowleft & \updownarrow \\ R^t & \underset{A}{\longrightarrow} & R^s & \underset{B}{\longrightarrow} & R^r \end{array}$$

(4.42) Corollary: (viz. 1026)
Let $(R,+,\cdot)$ be a commutative ring and consider two R-modules M and N which are free and finitely generated and let $s := \dim(M)$ and $r := \dim(N)$. Then we obtain the following statements:

(i) Let $\varphi : M \to N$ be a homomorphism of R-modules. Then the following three statements are equivalent (and in this case we already have $r = s$, of course)

 (a) φ is invertible (i.e. bijective)

 (b) There are some ordered bases $\mathcal{M}$ of M and $\mathcal{N}$ of N such that the matrix $[\varphi]^{\mathcal{N}}_{\mathcal{M}}$ is invertible.

 (c) For any two ordered bases $\mathcal{M}$ of M and $\mathcal{N}$ of N we find that the matrix $[\varphi]^{\mathcal{N}}_{\mathcal{M}}$ is invertible.

(ii) If $A \in \mathrm{mat}_s(R)$ is a square matrix, then the following two statements concerning A are equivalent

 (a) A is invertible

 (b) There are ordered bases $\mathcal{M}$, $\mathcal{M}'$ of M such that A is the matrix representation $A = [\mathbb{1}_M]^{\mathcal{M}'}_{\mathcal{M}}$ of the identity map $\mathbb{1}_M$ on M.

(iii) If $\mathcal{M} = (m_1, \ldots, m_s)$ is an ordered basis of M and $T = (t_{i,j}) \in \mathrm{mat}_s(R)$ is an invertible matrix, then we obtain another ordered basis $\mathcal{M}' = (m'_1, \ldots, m'_s)$ of M by letting (for any $i \in 1 \ldots s$)

$$m'_j \;:=\; \sum_{i=1}^{s} t_{i,j}\, m_i$$

 Nota thereby T becomes the matrix of the change of base from $\mathcal{M}'$ to $\mathcal{M}$. That is T transfers $\mathcal{M}'$ to $\mathcal{M}$ in the following sense: $T = [\mathbb{1}_M]^{\mathcal{M}}_{\mathcal{M}'}$ and $T^{-1} = [\mathbb{1}_M]^{\mathcal{M}'}_{\mathcal{M}}$ respectively.

(iv) If $\mathcal{M}$ and $\mathcal{M}'$ are ordered bases of M, likewise $\mathcal{N}$ and $\mathcal{N}'$ are ordered bases of N and $\varphi : M \to N$ is any homomorphism of R-modules, then we let $S := [\mathbb{1}_M]^{\mathcal{M}}_{\mathcal{M}'} \in \mathrm{mat}_s(R)$ and $T := [\mathbb{1}_N]^{\mathcal{N}'}_{\mathcal{N}} \in \mathrm{mat}_r(R)$. Thereby both S and T are invertible matrices and we find

$$[\varphi]^{\mathcal{N}'}_{\mathcal{M}'} \;=\; T\,[\varphi]^{\mathcal{N}}_{\mathcal{M}}\,S$$

(v) If $\varphi : M \to M$ is an endomorphism of the module M and $\mathcal{M}$, $\mathcal{M}'$ are ordered bases of M, then for $T := [\mathbb{1}_M]^{\mathcal{M}'}_{\mathcal{M}} \in \mathrm{mat}_s(R)$ we find

$$[\varphi]_{\mathcal{M}'} \;=\; T\,[\varphi]_{\mathcal{M}}\,T^{-1}$$

(4.43) Definition: $(\diamondsuit)$
Let $(R,+,\cdot)$ be a commutative ring, M be a free, finitely generated R-module and $\varphi \in \mathrm{end}(M)$ be an endomorphism of M. Then we may define the **trace** and **determinant** of φ by picking up *any* ordered basis $\mathcal{M} \subseteq M$ and using the trace and determinant of the matrix representation of φ:

$$\begin{aligned} \mathrm{tr}(\varphi) &:= \mathrm{tr}\,([\varphi]_{\mathcal{M}}) \\ \det(\varphi) &:= \det\,([\varphi]_{\mathcal{M}}) \end{aligned}$$

Prob We need to prove the well-definedness, that is given another ordered basis $\mathcal{M}' \subseteq M$ and letting $A := [\varphi]_{\mathcal{M}}$ and $A' := [\varphi]_{\mathcal{M}'}$ we need to check that $\mathrm{tr}(A') = \mathrm{tr}(A)$ and $\det(A') = \det(A)$ yield the same result. But by (4.42.(v)) there is some $T \in \mathrm{gl}_n(R)$ such that $A' = TAT^{-1}$. Therefore by (4.8.(v)) we have $\mathrm{tr}(A') = \mathrm{tr}(TAT^{-1}) = \mathrm{tr}(ATT^{-1}) = \mathrm{tr}(A)$ and by (4.55.(ii)) also $\det(A') = \det(TAT^{-1}) = \det(T)\det(A)\det(T)^{-1} = \det(A)$.

(4.44) Definition:
Let $(R, +, \cdot)$ be a commutative ring and $1 \leq m, n \in \mathbb{N}$. Then two matrices A and $B \in \mathrm{mat}_{m,n}(R)$ are said to be **equivalent** iff there are invertible matrices $S \in \mathrm{gl}_m(R)$ and $T \in \mathrm{gl}_n(R)$ such that

$$A \sim B \quad :\Longleftrightarrow \quad B = SAT$$

Moreover two square matrices A, $B \in \mathrm{mat}_n(R)$ are said to be **similar** iff there is an invertible matrix $T \in \mathrm{gl}_n(R)$ such that

$$A \approx B \quad :\Longleftrightarrow \quad B = TAT^{-1}$$

(4.45) Corollary: (viz. 1028)
If $(R, +, \cdot)$ is a commutative ring, $1 \leq m, n \in \mathbb{N}$ and $A, B \in \mathrm{mat}_{m,n}(R)$ we get the following statements

(i) The equivalence $\sim$ of matrices is an equivalence relation on the set $\mathrm{mat}_{m,n}(R)$ of $(m \times n)$-matrices over R. Thereby $A \sim B$ are equivalent, if and only if there is R-linear map $\varphi : R^n \to R^m$ and there are some ordered bases $\mathcal{M}$, $\mathcal{M}'$ of R^m and $\mathcal{N}$, $\mathcal{N}'$ of R^n respectively, such that

$$A = [\varphi]_{\mathcal{N}}^{\mathcal{M}} \quad \text{and} \quad B = [\varphi]_{\mathcal{N}'}^{\mathcal{M}'}$$

(ii) The similarity $\approx$ of matrices is an equivalence relation on the set $\mathrm{mat}_n(R)$ of $(n \times n)$-matrices over R. Thereby $A \approx B$ are similar, if and only if there is R-linear map $\varphi : R^n \to R^n$ and there are some ordered bases $\mathcal{M}$ and $\mathcal{N}$ of R^n such that

$$A = [\varphi]_{\mathcal{M}} \quad \text{and} \quad B = [\varphi]_{\mathcal{N}}$$

(iii) If $B = SAT$ for some invertible matrices $S \in \mathrm{gl}_m(R)$ and $T \in \mathrm{gl}_n(R)$, then the kernel and image of A and B satisfy the following relations

$$\begin{aligned} \mathrm{im}(B) &= S\,\mathrm{im}(A) \\ \mathrm{kn}(B) &= T^{-1}\,\mathrm{kn}(A) \end{aligned}$$

(4.46) Proposition: (viz. 1029)
Let $(R, +, \cdot)$ be a commutative ring and let M be a (free, finitely generated) R-module having the ordered basis $\mathcal{M} = (m_1, \ldots, m_n) \subseteq M$. Finally consider $\varphi \in \mathrm{end}(M)$ an R-module endomorphism on M and let $A := [\varphi]_{\mathcal{M}}$ be the matrix representation of φ. Then the following statements are not much of a surprise:

(i) Fix $r \in 1 \in 1 \ldots n$ and let $s := n - r$, consider the sub-module $P := \mathrm{Lh}\{\, m_1, \ldots, m_r \,\}$ and partition A into blocks the $A_{1,1} \in \mathrm{mat}_r(R)$, $A_{1,2} \in \mathrm{mat}_{r,s}(R)$, $A_{2,1} \in \mathrm{mat}_{s,r}(R)$ and finally $A_{2,2} \in \mathrm{mat}_s(R)$. That is A is decomposed into

$$A \;=\; \begin{pmatrix} A_{1,1} & A_{1,2} \\ A_{2,1} & A_{2,2} \end{pmatrix}$$

Then P is *invariant* under φ if and only if this block decomposition of A is upper triangular. Formally that is the following equivalence

$$\varphi(P) \;\subseteq\; P \quad\Longleftrightarrow\quad A_{2,1} \;=\; 0 \;\in\; \mathrm{mat}_{n-r,r}(R)$$

(ii) Let M^1, M^2, N^1 and N^2 all be R-modules having the ordered basis $\mathcal{M}^k = (m^k_1, \ldots, m^k_{r(k)}) \subseteq M^k$ and $\mathcal{N}^k = (n^k_1, \ldots, n^k_{s(k)}) \subseteq N^k$ respectively, where $k = 1$ or $k = 2$. We use these to build up ordered bases of $M := M^1 \oplus M^2$ and $N := N^1 \oplus N^2$ respectively:

$$\begin{aligned} \mathcal{M} &:= \Big((m^1_1, 0), \ldots, (m^1_{r(1)}, 0), (0, m^2_1), \ldots, (0, m^2_{r(2)}) \Big) \\ \mathcal{N} &:= \Big((n^1_1, 0), \ldots, (n^1_{s(1)}, 0), (0, n^2_1), \ldots, (0, n^2_{s(2)}) \Big) \end{aligned}$$

Also consider some R-module homomorphisms $\varphi_k : N^k \to M^k$ where $k = 1$ or $k = 2$ again. Then the basis representation of $\varphi_1 \oplus \varphi_2 : N \to M$ is the block diagonal matrix of basis representation of φ_1 and φ_2 respectively. In formal terms

$$[\varphi_1 \oplus \varphi_2]^{\mathcal{M}}_{\mathcal{N}} \;=\; \begin{pmatrix} [\varphi_1]^{\mathcal{M}^1}_{\mathcal{N}^1} & 0 \\ 0 & [\varphi_2]^{\mathcal{M}^2}_{\mathcal{N}^2} \end{pmatrix}$$

(iii) Recall that A is some matrix representation of the R-module endomorphism φ and consider any $r \in \mathbb{N}$ and $k(i) \in \mathbb{N}$ (where $i \in 1 \ldots r$) such that $\mathrm{rank}(M) = k(1) + \cdots + k(r)$. Then the following two statements are equivalent

(a) M is the inner direct sum of r free R-sub-modules $M_i \;\leq_{\mathrm{m}}\; M$ of $\mathrm{rank}(M_i) = k(i)$ that are invariant $\varphi(M_i) \subseteq M_i$ under φ, formally: $M \;=\; M_1 \oplus \cdots \oplus M_r$

(b) There are r square matrices $A_i \in \mathrm{mat}_{k(i)}(R)$ of size $k(i)$, such that A is similar to the block diagonal matrix of the A_i, formally: $A \;\approx\; A_1 \oplus \cdots \oplus A_r$

(4.47) Proposition: (viz. 1030)
Let $(R, +, \cdot)$ be a commutative ring and consider two R-modules M and N with the ordered bases $\mathcal{M} = (m_1, \ldots, m_s)$ of M and $\mathcal{N} = (n_1, \ldots, n_r)$ of N respectively. Then we obtain a 1-to-1 correspondence between the bilinear forms $b : M \oplus N \to R$ and the $(r \times s)$-matrices over R, given by

$$\begin{aligned} \{\, b : M \oplus N \to R \mid b \text{ is bilinear} \,\} &\longleftrightarrow \mathrm{mat}_{r,s}(R) \\ b &\mapsto \big(b(m_j, n_i)\big) \\ \Big((x, y) \mapsto \langle B[x]_{\mathcal{M}}, [y]_{\mathcal{N}} \rangle\Big) &\hookleftarrow B \end{aligned}$$

In case $M = N$ (and $\mathcal{M} = \mathcal{N}$) a bilinear form $b : M \oplus M \to R$ is said to be *symmetric*, iff for any x, $y \in M$ we have $b(x,y) = b(y,x)$. Likewise a matrix $B \in \mathrm{mat}_r(R)$ is said to be *symmetric* iff $B = B^*$. Now if $B = (b(m_j, m_i))$ is the matrix corresponding to the bilinear form b, then b is symmetric if and only if B is such:

$$b \text{ is symmetric} \quad \Longleftrightarrow \quad B \text{ is symmetric}$$

(4.48) Remark:
Note that *bilinear* means that $b : M \oplus N \to R$ is *multi-linear*, where the *bi-* refers to the fact that its preimage is composed of two modules. That is for any $a \in R$ and any x, $x' \in M$, y, $y' \in N$ we have $b(ax + x', y) = ab(x,y) + b(x',y)$ and $b(x, ay + y') = ab(x,y) + b(x,y')$. The word *form* is used for maps whose image lies in the base ring R again.

(4.49) Remark:
A map q of the form $q : M \oplus M \to R$ is said to be a *quadratic form* iff there is some bilinear form $b : M \oplus M \to R$ such that for any $x \in M$ we get $q(x) = b(x,x)$. Thus if we fix an ordered basis $\mathcal{M} = (m_1, \ldots, m_r)$ of M then this means that there is some matrix $B \in \mathrm{mat}_r(R)$ such that

$$q(x) \quad = \quad \langle B[x]_{\mathcal{M}}, [x]_{\mathcal{M}} \rangle$$

Thereby $B = (b_{i,j})$ is given to be $b_{i,j} = b(m_j, m_i)$. If we now take $u = (u_1, \ldots, u_r) \in R^r$ to be the basis representation $u = [x]_{\mathcal{M}}$ of $x \in M$ then we immediately find an explicit representation of q:

$$q(x) \quad = \quad \sum_{i=1}^{r} b_{i,i} u_i^2 + \sum_{i<j} (b_{i,j} + b_{j,i}) u_i u_j$$

In other words: If q is a quadratic form, then there are some coefficients $b_{i,j} \in R$ such that the above equation holds. And conversely for any $b_{i,j} \in R$ the above equation defines a quadratic form.

4.5 Determinants

In this section we will introduce the most fundamental notion of a *determinant*, $\det(A)$ of a square matrix A, which will be a criterion for the invertibility of A and hence the solvability of a square system of linear equations. In a more general setting the determinant is an example of *quantifier elimination*: We will find the equivalence

$$\exists\, B \in \mathrm{mat}_n(R) \;:\; AB = \mathbb{1}_n \quad \Longleftrightarrow \quad \det(A) \in R^*$$

Thereby the left-hand side of this equivalence contains an existential quantifier, thus it's hard to check, whether this property is satisfied. The right-hand side however contains no quantifiers and hence is straightforward to check. That's what makes the determinant so powerful.
But there's even more to the determinant: In the previous section we have introduced the Gauss-algorithm that can be used to solve systems of linear equations. This algorithm works like charm for any given SLE, but it can only be applied to one SLE at a time. It lacks a general theory of how the solution is obtained. Cramer's rule will be precisely this: A formula how the solution can be computed, an it will be formulated in terms of determinants. This theorem is the staging point for a lot of other powerful theorems, as it enables us to give computational answers to structural questions.
In order to see how all this comes about let us regard the most simple non-trivial system of linear equations, a system of size 2×2 in general form, say

$$\begin{aligned} a_{1,1}x_1 + a_{1,2}x_2 &= b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 &= b_2 \end{aligned}$$

In this setting the determinant, Cramer's rule and everything else can be seen in an elementary way. The easiest way to solve this SLE is to multiply the upper equation by $a_{2,1}$ and the lower equation by $a_{1,1}$

$$\begin{aligned} a_{2,1}a_{1,1}x_1 + a_{2,1}a_{1,2}x_2 &= a_{2,1}b_1 \\ a_{1,1}a_{2,1}x_1 + a_{1,1}a_{2,2}x_2 &= a_{1,1}b_2 \end{aligned}$$

If R is a commutative ring we have $a_{2,1}a_{1,1} = a_{1,1}a_{2,1}$ and hence we eliminate the variable x_1 by subtracting the upper from the lower equation. This leaves

$$(a_{1,1}a_{2,2} - a_{2,1}a_{1,2})\, x_2 \;=\; a_{1,1}b_2 - a_{2,1}b_1$$

Here we have found the so-called *determinant* of A, it is the element $d := a_{1,1}a_{2,2} - a_{2,1}a_{1,2} \in R$. It can be computed for any 2×2 matrix and we will introduce the notation

$$\det \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} \;:=\; a_{1,1}a_{2,2} - a_{2,1}a_{1,2}$$

Now, if d is an invertible element of R, then we have found a formula for the solution x_2 (and in complete analogy we find a similar formula for x_1).

$$\begin{aligned} x_1 &= d^{-1} \cdot (a_{2,2}b_1 - a_{1,2}b_2) &= d^{-1} \cdot \det \begin{pmatrix} b_1 & a_{1,2} \\ b_2 & a_{2,2} \end{pmatrix} \\ x_2 &= d^{-1} \cdot (a_{1,1}b_2 - a_{2,1}b_1) &= d^{-1} \cdot \det \begin{pmatrix} a_{1,1} & b_1 \\ a_{2,1} & b_2 \end{pmatrix} \end{aligned}$$

This already is Cramer's rule in the 2×2 case: The solution of a SLE can be expressed in terms of determinants. It can be generalized to SLEs of arbitrary size, but this will first require a generalization of the determinant for larger matrices. This is quite a strong result: If $d = a_{1,1}a_{2,2} - a_{2,1}a_{1,2}$ is invertible, then the whole matrix is invertible. And looking at the formulas for x_1 and x_2 above we even see the inverse matrix of A:

$$\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}^{-1} = d^{-1} \cdot \begin{pmatrix} a_{2,2} & -a_{1,2} \\ -a_{2,1} & a_{1,1} \end{pmatrix}$$

More generally - if we ignore d for a minute - we have found another matrix (the so-called *adjugate* matrix) that is an inverse up to the determinant d as a factor

$$\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} \begin{pmatrix} a_{2,2} & -a_{1,2} \\ -a_{2,1} & a_{1,1} \end{pmatrix} = d \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

So if $d \in R$ is a unit in R, then A has an inverse matrix. But the converse statement is true, as well: In case 2×2 it is a lengthy, but elementary computation, to show that $\det(AB) = \det(A) \cdot \det(B)$. We skip this, as we will prove it for determinants of any size. However if A has an inverse matrix A^{-1} it follows, that the determinant of A has to be a unit of R, since

$$1 = \det(\mathbb{1}_2) = \det(AA^{-1}) = \det(A) \cdot \det(A^{-1})$$

Thus we have proved the above equivalence for the case of 2×2 matrices. And along the way we have seen Cramer's rule and the adjugate matrix of a matrix.

In the general case of arbitrary size the arguments will follow precisely the same line, all we have to do is define the determinant and then prove that it has some nice properties that enable us to the same computations in the general setting.

For the definition we will require the notion of a permutation, though. This is a bijective map $\sigma : 1 \dots n \longleftrightarrow 1 \dots n$. We have already studied the group S_n of all permutations of n elements in section 1.2 and seen that this contains precisely $\#S_n = n!$ elements. Any permutation can be decomposed into transpositions. This decomposition is not unique, but the number of transpositions required always is either odd or even. In case of an even number we set $\operatorname{sgn}(\sigma) = 1$ and in case of an odd number we set $\operatorname{sgn}(\sigma) = -1$. This is the basis for the following definition:

(4.50) Definition:
Let $(R,+,\cdot)$ be a commutative ring and $1 \leq n \in \mathbb{N}$ a natural number. If now A is an $(n \times n)$-matrix having the coefficients

$$A \;=\; \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \vdots & & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \dots & a_{n,n} \end{pmatrix}$$

then we define the **determinant** of A explicitly, to be the following element of R: (note that this definition makes sense, since the sum runs over the *finite* set S_n of all permutations on $1 \dots n$)

$$\det(A) \;:=\; \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}$$

(4.51) Example:
In case $n = 2$ there are precisely two permutations: the identity $\mathbb{1}$ and the transposition $(1\,2)$. Thereby the determinant has two summands only, in this case

$$\det(A) \;=\; a_{1,1}a_{2,2} - a_{1,2}a_{2,1}$$

In case $n = 3$ there are 6 permutations: The even permutations $\mathbb{1}$, $(1\,2\,3)$ and $(1\,3\,2)$ and the transpositions (hence odd permutations) $(1\,2)$, $(1\,3)$ and $(2\,3)$. Therefore - in this case - the determinant is given to be

$$\begin{aligned} \det(A) \;=\; & a_{1,1}a_{2,2}a_{3,3} + a_{1,2}a_{2,3}a_{3,1} + a_{1,3}a_{2,1}a_{3,2} \\ & -a_{1,2}a_{2,1}a_{3,3} - a_{1,3}a_{2,2}a_{3,1} - a_{1,1}a_{2,3}a_{3,2} \end{aligned}$$

Our last example will be $n = 4$: Here S_4 already contains $4! = 24$ permutations. Beyond that it would be tedious to try to write out the determinant explicitly and we have to use other means to evaluate it - namely the expansion theorems of Laplace. For $n = 4$ there are 12 even permutations: The identity $\mathbb{1}$, 8 3-cycles and 3 pairs of transpositions and another 12 odd permutations: 6 transpositions and 6 4-cycles, altogether:

$$\begin{aligned} \det(A) \;=\; & a_{1,1}a_{2,2}a_{3,3}a_{4,4} + a_{1,1}a_{2,3}a_{3,4}a_{4,2} + a_{1,1}a_{2,4}a_{3,2}a_{4,3} \\ & +a_{1,3}a_{2,2}a_{3,4}a_{4,1} + a_{1,4}a_{2,2}a_{3,1}a_{4,3} + a_{1,2}a_{2,4}a_{3,3}a_{4,1} \\ & +a_{1,4}a_{2,1}a_{3,3}a_{4,2} + a_{1,2}a_{2,3}a_{3,1}a_{4,4} + a_{1,3}a_{2,1}a_{3,2}a_{4,4} \\ & +a_{1,2}a_{2,1}a_{3,4}a_{4,3} + a_{1,3}a_{2,4}a_{3,1}a_{4,2} + a_{1,4}a_{2,3}a_{3,2}a_{4,1} \\ & -a_{1,1}a_{2,2}a_{3,4}a_{4,3} - a_{1,1}a_{2,4}a_{3,3}a_{4,2} - a_{1,1}a_{2,3}a_{3,2}a_{4,4} \\ & -a_{1,4}a_{2,2}a_{3,3}a_{4,1} - a_{1,3}a_{2,2}a_{3,1}a_{4,4} - a_{1,2}a_{2,1}a_{3,3}a_{4,4} \\ & -a_{1,2}a_{2,3}a_{3,4}a_{4,1} - a_{1,2}a_{2,4}a_{3,1}a_{4,3} - a_{1,3}a_{2,1}a_{3,4}a_{4,2} \\ & -a_{1,3}a_{2,4}a_{3,2}a_{4,1} - a_{1,4}a_{2,3}a_{3,1}a_{4,2} - a_{1,4}a_{2,1}a_{3,2}a_{4,3} \end{aligned}$$

(4.52) Definition:
Let $(R,+,\cdot)$ be a commutative ring and $1 \leq n \in \mathbb{N}$ a natural number. Let us now regard a map of the following form

$$D \;:\; \Big(R^n\Big)^n \to R \;:\; (a_1, a_2, \ldots, a_n) \mapsto D(a_1, a_2, \ldots, a_n)$$

We have already defined what it means that D is R-multi-linear: Namely iff for any $a_1, \ldots, a_n \in R^n$, any $x, y \in R^n$ any $b \in R$ and any $j \in 1 \ldots n$ we get

$$\begin{aligned} D(\ldots, a_{j-1}, x+y, a_{j+1}, \ldots) &= D(\ldots, a_{j-1}, x, a_{j+1}, \ldots) + D(\ldots, a_{j-1}, y, a_{j+1}, \ldots) \\ D(\ldots, a_{j-1}, ba_j, a_{j+1}, \ldots) &= bD(\ldots, a_{j-1}, a_j, a_{j+1}, \ldots) \end{aligned}$$

In this case D is said to be a **multi-linear form**, where *form* refers to fact that D maps to the base ring R. Now D is said to be **alternating** iff for any $a_1, \ldots, a_n \in R^n$ and any permutation $\sigma \in S_n$ we get

$$D(a_{\sigma(1)}, a_{\sigma(2)}, \ldots, a_{\sigma(n)}) \;=\; \operatorname{sgn}(\sigma) D(a_1, a_2, \ldots, a_n)$$

And finally D is said to be a **determinant form**, iff it is R-multi-linear and for any $a_1, \ldots, a_n \in R^n$ and any $i \neq j \in 1 \ldots n$ we get the implication

$$a_i \;=\; a_j \quad\Longrightarrow\quad D(a_1, a_2, \ldots, a_n) \;=\; 0$$

(4.53) Remark:

(i) As always we canonically identify the set $(R^n)^n$ of n n-tuples over R with the set of $(n \times n)$-matrices, by taking to the column-vectors of a matrix A. That is we consider $A = (a_1, a_2, \ldots, a_n)$ where the $a_i \in R^n$ are the column vectors of A

$$\begin{array}{rcl} \operatorname{mat}_n(R) & \longleftrightarrow & \Big(R^n\Big)^n \\ A & \mapsto & \Big(\operatorname{col}_1(A), \operatorname{col}_2(A), \ldots, \operatorname{col}_n(A)\Big) \\ \begin{pmatrix} \vdots & \vdots & & \vdots \\ a_1 & a_2 & \ldots & a_n \\ \vdots & \vdots & & \vdots \end{pmatrix} & \mapsfrom & (a_1, a_2, \ldots, a_n) \end{array}$$

In particular if D is a multi-linear form and A is a matrix of appropriate size, then $D(A) \in R$ is just D applied to the columns of A

$$D(A) \;=\; D\Big(\operatorname{col}_1(A), \operatorname{col}_2(A), \ldots, \operatorname{col}_n(A)\Big)$$

(ii) In the definition of the determinant (4.50) we used terms of the form $a_{1,\sigma(1)} a_{2,\sigma(2)} \ldots a_{n,\sigma(n)} \in R$. Note that letting $j := \sigma(i) \in 1 \ldots n$ the entry $a_{i,\sigma(i)}$ of A can also be addressed, as

$$a_{i,\sigma(i)} \;=\; a_{\sigma^{-1}(j),j}$$

Since R is commutative, the product runs over all $i \in 1 \dots n$ and σ is bijective, we can as well multiply over all $j = \sigma(i) \in 1 \dots n$, such that

$$\prod_{i=1}^{n} a_{i,\sigma(i)} \;=\; \prod_{j=1}^{n} a_{\sigma^{-1}(j),j}$$

Thus if the matrix $A = (a_{i,j})$ has the column vectors $a_j = \mathrm{col}_j(A) = (a_{1,j}, a_{2,j}, \dots, a_{n,j}) \in R^n$ then the determinant can be rewritten, as

$$\begin{aligned} \det(A) &= \det(a_1, a_2, \dots, a_n) \\ &= \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)} \\ &= \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \prod_{j=1}^{n} a_{\sigma^{-1}(j),j} \end{aligned}$$

That is $\det(a_1, a_2, \dots, a_n)$ selects the $\sigma^{-1}(j)$-th entry $a_{\sigma^{-1}(j),j}$ from the j-th vector a_j and sums up all these products. This may be a little awkward, but is ultimately due to the convention that in $A = (a_{i,j})$ the index i enumerates the row and j enumerates the column.

(iii) The online computer algebra system Wolfram α can also deal with vectors, matrices and compute determinants. Since this program is operated by command line, it stands to reason that it uses row-vectors. The input {x_1,x_2, x_3} is interpreted as the triple $x = (x_1, x_{2,3}) \in R^3$ for example. Likewise {{a_11,a_12, a_23}, {a_21, a_22, a_23}, {a_31, a_32, a_33}} denotes the matrix $A = (a_{ij}) \in \mathrm{mat}_3(R)$ whose row vectors are given to be $\mathrm{row}_i(A) = (a_{i1}, a_{i2}, a_{i3})$. Of course Wolfram α can handle higher (and lower) dimensions, as well.

(iv) If C and D are multi-linear forms and $a \in R$ is a scalars, then it is clear, that both aD and $C + D$ are a multi-linear forms, as well. That is the set of all multi-linear forms (of the same size) is an R-module under the point-wise operations

$$\begin{aligned} aD &: \mathrm{mat}_n(R) \to R \;:\; A \mapsto a \cdot D(A) \\ C + D &: \mathrm{mat}_n(R) \to R \;:\; A \mapsto C(A) + D(A) \end{aligned}$$

(v) If any $a_j \in R^n$ is given to be $a_j = (a_{1,j}, a_{2,j}, \dots, a_{n,j})$ and $\sigma \in S_n$ is any fixed permutation, then it is easy to check, that

$$D(a_1, a_2, \dots, a_n) \;:=\; a_{\sigma(1),1} a_{\sigma(2),2} \dots a_{\sigma(n),n}$$

is a multi-linear form. Therefore, if $r : S_n \to R$ is any map that assigns every permutation $\sigma \in S_n$ a scalar $r(\sigma) \in R$, then due to (iv) we obtain a multi-linear form, by letting

$$D(a_1, a_2, \dots, a_n) \;:=\; \sum_{\sigma \in S_n} r(\sigma)\, a_{\sigma(1),1} a_{\sigma(2),2} \dots a_{\sigma(n),n}$$

(4.54) Proposition: (viz. 851)
Let $(R, +, \cdot)$ be a commutative ring, $2 \leq n \in \mathbb{N}$ and $D : \mathrm{mat}_n(R) \to R$ be a multi-linear form over R. If now $2 = 1 + 1 \in \mathrm{NZD}(R)$ is a non-zero divisor of R, then the following three statements are equivalent:

(a) D is a determinant form: For any $a_1, \ldots, a_n \in R^n$ and any $i \neq j \in 1 \ldots n$ we get the implication

$$a_i \;=\; a_j \quad\Longrightarrow\quad D(a_1, a_2, \ldots, a_n) \;=\; 0$$

(b) D is alternating: For any $a_1, \ldots, a_n \in R^n$ and any permutation $\sigma \in S_n$ we get the equality of

$$D(a_{\sigma(1)}, a_{\sigma(2)}, \ldots, a_{\sigma(n)}) \;=\; \operatorname{sgn}(\sigma) D(a_1, a_2, \ldots, a_n)$$

(c) For any $a_1, \ldots, a_n \in R^n$ and any transposition $\tau \in S_n$ [that is $\tau = (i\,j)$ for some $i \neq j \in 1 \ldots n$] we get the following equality

$$D(a_{\tau(1)}, a_{\tau(2)}, \ldots, a_{\tau(n)}) \;=\; -D(a_1, a_2, \ldots, a_n)$$

Generally - for an arbitrary commutative ring - statement (a) is not equivalent, to (c), but (c) still implies $2D(a_1, a_2, \ldots, a_n) = 0$. Therefore in general we find

$$\text{(a)} \quad\Longrightarrow\quad \text{(b)} \quad\Longleftrightarrow\quad \text{(c)}$$

And if $D : \mathrm{mat}_n(R) \to R$ is a determinant form over some integral domain R, then for any n vectors a_1, $a_2, \ldots, a_n \in R^n$ we find the following implication

$$\{\, a_1, a_2, \ldots, a_n \,\} \text{ linearly dependent} \quad\Longrightarrow\quad D(a_1, a_2, \ldots, a_n) \;=\; 0$$

If $D : \mathrm{mat}_n(R) \to R$ is a determinant form over some non-zero, commutative ring $R \neq 0$ only, then for any n vectors a_1, $a_2, \ldots, a_n \in R^n$ we still find the implication

$$\operatorname{ann}\big(D(a_1, a_2, \ldots, a_n)\big) \;=\; 0 \quad\Longrightarrow\quad \{\, a_1, a_2, \ldots, a_n \,\} \text{ linearly independent}$$

(4.55) Lemma: (viz. 852)
Let $(R, +, \cdot)$ be a commutative ring, $1 \leq n \in \mathbb{N}$ and consider the determinant $\det : \mathrm{mat}_n(R) \to R$ defined in (4.50). Then this determinant satifies a couple of noteworthy properties:

(i) If $A \in \mathrm{mat}_n(R)$ is a matrix and A^* denotes the transpose of A, then both A and A^* share the same determinant, formally that is

$$\det(A^*) \;=\; \det(A)$$

(ii) The determinant is a homomorphism from the (non-commutative) monoid of matrices (under multiplication) to the (commutative) monoid of R under multiplication. I.e. for the identity matrix $\mathbb{1}_n \in \mathrm{mat}_n(R)$ and any two matrices $A, B \in \mathrm{mat}_n(R)$ we get

$$\begin{aligned} \det(\mathbb{1}_n) &= 1 \\ \det(AB) &= \det(A) \cdot \det(B) \end{aligned}$$

(iii) The determinant $\det : \mathrm{mat}_n(R) \to R$ is a determinant form, i.e. a multi-linear map, such that for

any matrix $A \in \mathrm{mat}_n(R)$ that has two identical columns the determinant is zero, i.e.

$$\exists\, i \neq j \in 1 \ldots n \;:\; \mathrm{col}_i(A) \;=\; \mathrm{col}_j(A) \quad\Longrightarrow\quad \det(A) \;=\; 0$$

(iv) If $D : \mathrm{mat}_n(R) \to R$ is any other determinant form on R, then D already is a multiple of the determinant. I.e. for any $A \in \mathrm{mat}_n(R)$ we get the following equality

$$D(A) \;=\; D(\mathbb{1}_n) \cdot \det(A)$$

(v) **Laplace expansion theorem**: Let $A \in \mathrm{mat}_n(R)$ be any square matrix over R and for any p, $q \in 1 \ldots n$ let us denote the matrix in which the p-th row and q-th column are scratched from A by $A_{p,q}$:

$$A_{p,q} \;=\; \begin{pmatrix} a_{1,1} & a_{1,2} & \ldots & a_{1,q-1} & a_{1,q+1} & \ldots & a_{1,n} \\ a_{2,1} & a_{2,2} & \ldots & a_{2,q-1} & a_{2,q+1} & \ldots & a_{2,n} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ a_{p-1,1} & a_{p-1,2} & \ldots & a_{p-1,q-1} & a_{p-1,q+1} & \ldots & a_{p-1,n} \\ a_{p+1,1} & a_{p+1,2} & \ldots & a_{p+1,q-1} & a_{p+1,q+1} & \ldots & a_{p+1,n} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ a_{n,1} & a_{n,2} & \ldots & a_{n,q-1} & a_{n,q+1} & \ldots & a_{n,n} \end{pmatrix}$$

More formally let us define the maps α and $\beta : 1 \ldots (n-1) \to 1 \ldots n$ by $\alpha(i) := i$ if $i < p$ and $\alpha(i) := i+1$ if $i \geq p$ respectively by $\beta(j) := j$ if $j < q$ and $\beta(i) := j+1$ if $j \geq q$. Then $A_{p,q}$ is the following matrix

$$A_{p,q} \;:=\; \Big(a_{\alpha(i),\beta(j)}\Big)_{i,j \in 1\ldots(n-1)} \;\in\; \mathrm{mat}_{n-1}(R)$$

Now fix any $p \in 1 \ldots n$, then we can evaluate the determinant of A by *expansion along the p-th row* of A, in the following sense

$$\det(A) \;=\; \sum_{q=1}^{n} (-1)^{p+q} a_{p,q} \det\big(A_{p,q}\big)$$

Likewise fix any $q \in 1 \ldots n$, then we can evaluate the determinant of A by *expansion along the q-th column* of A, in the following sense

$$\det(A) \;=\; \sum_{p=1}^{n} (-1)^{p+q} a_{p,q} \det\big(A_{p,q}\big)$$

(vi) Let $(S, +, \cdot)$ be another commutative ring and $\alpha : R \to S$ be a homomorphism of rings. For a matrix $A = (a_{i,j}) \in \mathrm{mat}_n(R)$ let us denote $\alpha(A) := (\alpha(a_{i,j})) \in \mathrm{mat}_n(S)$. Then the determinant of $\alpha(A)$ is

$$\det\big(\alpha(A)\big) \;=\; \alpha\big(\det(A)\big)$$

(4.56) Remark:
It is worth to note that the above lemma has some immediate consequences: Since the determinant is linear in every column of $A \in \mathrm{mat}_n(R)$ it is clear, that whenever a single column of A vanishes, so does the determinant:

$$\exists\, j \in 1 \ldots n \;:\; \mathrm{col}_j(A) = 0 \quad \Longrightarrow \quad \det(A) \;=\; 0$$

Of course this is also clear from the definition of det itself, as every product then contains at least one 0. Also if A contains a row, that is 0, then A^* contains a column, that is 0. But as A and A^* share the same determinant, we likewise find

$$\exists\, i \in 1 \ldots n \;:\; \mathrm{row}_i(A) = 0 \quad \Longrightarrow \quad \det(A) \;=\; 0$$

Again, this is also clear from the explicit formula of the determinant. Furthermore since det is a determinant form, (4.54) tells us, that det also is alternating. That is, permuting the columns of A just changes the sign of the determinant

$$\det \begin{pmatrix} | & & | \\ a_{\sigma(1)} & \cdots & a_{\sigma(n)} \\ | & & | \end{pmatrix} \;=\; \mathrm{sgn}(\sigma) \cdot \det \begin{pmatrix} | & & | \\ a_1 & \cdots & a_n \\ | & & | \end{pmatrix}$$

Likewise transposing A permuting the columns of A^* and transposing again, is just the same as permuting the rows of A. But since transposing does not change the determinant, we also see that

$$\det \begin{pmatrix} — & a_{\sigma(1)} & — \\ & \vdots & \\ — & a_{\sigma(n)} & — \end{pmatrix} \;=\; \mathrm{sgn}(\sigma) \cdot \det \begin{pmatrix} — & a_1 & — \\ & \vdots & \\ — & a_n & — \end{pmatrix}$$

(4.57) Example:
The easiest application of the Laplace expansion theorem is the case $n = 2$. That is we want to compute the determinant of the general (2×2)-matrix

$$A \;=\; \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}$$

We choose $p = 1$ that is we will expand the determinant along the first row of A. As for an $a \in R$ we trivially have $\det(a) = a$ this quickly yields the same formula we encountered in the example before

$$\det \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} \;=\; a_{1,1}\det(a_{2,2}) - a_{1,2}\det(a_{2,1}) \;=\; a_{1,1}a_{2,2} - a_{1,2}a_{2,1}$$

More instructive is the case $n = 3$, that is we want to compute the determinant of the general (3×3)-matrix

$$A \;=\; \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}$$

Let us choose $q = 2$, that is we will expand the determinant along the middle column of A - there is no

special reason for this choice, apart from emphasizing that it can be done. Then the Laplace expansion theorem yields

$$\det\begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix} = -a_{1,2}\det\begin{pmatrix} a_{2,1} & a_{2,3} \\ a_{3,1} & a_{3,3} \end{pmatrix} + a_{2,2}\det\begin{pmatrix} a_{1,1} & a_{1,3} \\ a_{3,1} & a_{3,3} \end{pmatrix} - a_{3,2}\det\begin{pmatrix} a_{1,1} & a_{1,3} \\ a_{2,1} & a_{2,3} \end{pmatrix}$$

And using the formula for the determinants of those (2×2)-matrices we wind up with precisely the same formula, we found while looking at permutations

$$\begin{aligned} \det\begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix} &= -a_{1,2}\left(a_{2,1}a_{3,3} - a_{2,3}a_{3,1}\right) \\ &\quad +a_{2,2}\left(a_{1,1}a_{3,3} - a_{1,3}a_{3,1}\right) \\ &\quad -a_{3,2}\left(a_{1,1}a_{2,3} - a_{1,3}a_{2,1}\right) \\ &= -a_{1,2}a_{2,1}a_{3,3} - a_{1,3}a_{2,2}a_{3,1} - a_{1,1}a_{2,3}a_{3,2} \\ &\quad +a_{1,2}a_{2,3}a_{3,1} + a_{1,1}a_{2,2}a_{3,3} + a_{1,3}a_{2,1}a_{3,2} \end{aligned}$$

The Laplace expansion theorem yields an algorithm to compute the determinant of any square matrix by recursion. Though this is a vast progress compared to the definition, it can result in an excessively long computation, that we would like to evade, still. However there are two major cases in which the computation of the determinant is easily feasible:

(4.58) Proposition: (viz. 858)
Let $(R, +, \cdot)$ be a commutative ring $1 \leq m$, $n \in \mathbb{N}$ and $A \in \mathrm{mat}_m(R)$ and B, $T = (t_{i,j}) \in \mathrm{mat}_n(R)$ be square matrices over R. Then we get

(i) Let also $C \in \mathrm{mat}_{m,n}(R)$ and $0 \in \mathrm{mat}_{n,m}$, then we can compute the trace and determinant of the following block matrix, using

$$\begin{aligned} \mathrm{tr}\begin{pmatrix} A & C \\ 0 & B \end{pmatrix} &= \mathrm{tr}(A) + \mathrm{tr}(B) \\ \det\begin{pmatrix} A & C \\ 0 & B \end{pmatrix} &= \det(A) \cdot \det(B) \end{aligned}$$

(ii) In particular the trace and determinant of a direct sum $A \oplus B$ of matrices can be computed for A and B separately, using

$$\begin{aligned} \mathrm{tr}(A \oplus B) &= \mathrm{tr}(A) + \mathrm{tr}(B) \\ \det(A \oplus B) &= \det(A) \cdot \det(B) \end{aligned}$$

(iii) If T is an lower triangular (i.e. $i < j \implies t_{i,j} = 0$) matrix or an upper triangular matrix (i.e. $i > j \implies t_{i,j} = 0$), then the determinant of T is just the product of its diagonal elements

$$\det(T) = \prod_{i=1}^{n} t_{i,i}$$

(4.59) Remark:
It generally is a reasonable strategy to use the Gaussian algorithm to bring a matrix $A \in \mathrm{mat}_n(R)$ into upper triangular form. The determinant of this matrix can then be computed using (ii). However the Gaussian algorithm makes use of elementary matrices, so we have to keep track how the determinant changes: If $\sigma \in S_n$ is any permutation, $a \in R$ is a scalar and $i \neq j \in 1 \ldots n$, then due to the multiplicativity of the determinant we get

$$\begin{aligned} \det\Big(P_\sigma A\Big) &= \mathrm{sgn}(\sigma)\det(A) \\ \det\Big(D_i(a)A\Big) &= a \cdot \det(A) \\ \det\Big(T_{i,j}(a)A\Big) &= \det(A) \end{aligned}$$

Let us regard an example of this method: Say we would like to compute the determinant of the following (3×3)-matrix over $\mathbb{Z}$.

$$A = \begin{pmatrix} 2 & 6 & 2 \\ 0 & 2 & 2 \\ 3 & 7 & 4 \end{pmatrix}$$

We aim to get A into upper triangular form. In order to get there we divide the first row by 2 and interchange the second and third rows, arriving at

$$A_1 = \begin{pmatrix} 1 & 3 & 1 \\ 3 & 7 & 4 \\ 0 & 2 & 2 \end{pmatrix}$$

Due to our operations we know, that $\det(A_1) = -1/2 \cdot \det(A)$. Next we subtract 3-times the first row from the second row, now getting to

$$A_2 = \begin{pmatrix} 1 & 3 & 1 \\ 0 & -2 & 1 \\ 0 & 2 & 2 \end{pmatrix}$$

Note that this did not change the determinant at all: $\det(A_2) = \det(A_1)$. Adding the the second row to the third row we arrive at the upper triangular form already

$$T = \begin{pmatrix} 1 & 3 & 1 \\ 0 & -2 & 1 \\ 0 & 0 & 3 \end{pmatrix}$$

Again this did not change the determinant $\det(T) = \det(A_2)$. Since T is triangular it is easy to compute it's determinant. And retracing our steps we thereby find the determinant of A

$$-6 = \det(T) = \det(A_2) = \det(A_1) = -\frac{1}{2}\det(A)$$

$$\Longrightarrow \quad \det(A) = (-2) \cdot (-6) = 12$$

Clearly the advantage of this method lies in the fact that it takes n steps to get A into upper triangular form. And from there the determinant is nothing but the product of the diagonal elements. Using the Laplace expansion theorem (for all its worth) requires to expand $n!$ times.

(4.60) Remark:
There is an easy way to prove statement (ii) in (4.58): Simply define the map $D : \mathrm{mat}_m(R) \to R$ by $D(A) := \det(A \oplus B)$. As det is linear in every argument, so is D. Also it is clear that D inherits being a determinant form from det. Finally it is not hard to see, that

$$D(\mathbb{1}_m) \;=\; \det(\mathbb{1}_m \oplus B) \;=\; \det(B)$$

Hence we may invoke (4.55.(iv)) to find that for any $A \in \mathrm{mat}_m(R)$ we have

$$\det(A \oplus B) \;=\; D(A) \;=\; \det(A) \cdot D(\mathbb{1}_m) \;=\; \det(A) \cdot \det(B)$$

However we chose to present a direct proof of this statement, in order to have more independence between proofs and as it is a natural reflex to split S_{m+n} into S_m and S_n when looking at the construction of $A \oplus B$.

In the expansion theorem of Laplace (4.55.(v)) we encountered the sub-matrices $A_{p,q}$ in which the p-th row and q-th column of A have been deleted. Even though these seem to be just a peculiarity of the expansion theorem, these can also be applied to solving systems of linear equations. In order to formulate Cramer's rule (which is a solution formula) we need to introduce some notation first:

(4.61) Definition:
Let $(R, +, \cdot)$ be a commutative ring and $2 \leq n \in \mathbb{N}$, if now $A = (a_{i,j})$ is a square matrix of size $(n \times n)$ and $p, q \in 1 \ldots n$ are some indexes we denote (as in the expansion theorem of Laplace) again

$$A_{p,q} \;=\; \begin{pmatrix} a_{1,1} & a_{1,2} & \ldots & a_{1,q-1} & a_{1,q+1} & \ldots & a_{1,n} \\ a_{2,1} & a_{2,2} & \ldots & a_{2,q-1} & a_{2,q+1} & \ldots & a_{2,n} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ a_{p-1,1} & a_{p-1,2} & \ldots & a_{p-1,q-1} & a_{p-1,q+1} & \ldots & a_{p-1,n} \\ a_{p+1,1} & a_{p+1,2} & \ldots & a_{p+1,q-1} & a_{p+1,q+1} & \ldots & a_{p+1,n} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ a_{n,1} & a_{n,2} & \ldots & a_{n,q-1} & a_{n,q+1} & \ldots & a_{n,n} \end{pmatrix}$$

the matrix A in which the p-th row and q-th column have been scratched. Formall we define the maps α and $\beta : 1 \ldots (n-1) \to 1 \ldots n$ by $\alpha(i) := i$ if $i < p$ and $\alpha(i) := i + 1$ if $i \geq p$ respectively by $\beta(j) := j$ if $j < q$ and $\beta(i) := j + 1$ if $j \geq q$. Then $A_{p,q}$ is the following matrix

$$A_{p,q} \;:=\; \left(a_{\alpha(i),\beta(j)}\right)_{i,j \in 1\ldots(n-1)} \;\in\; \mathrm{mat}_{n-1}(R)$$

Now the **cofactor matrix** $\mathrm{cof}(A)$ is defined to be the $(n \times n)$-matrix whose coefficients are (up to sign) the determinant of these $A_{p,q}$. The transpose of the cofactor matrix is said to be the **adjugate matrix** $A^{\#}$ of A. We also define these notions formally:

$$\begin{aligned} \mathrm{cof}(A) &:= \Big((-1)^{p+q} \det(A_{p,q}) \Big)_{p,q \in 1 \ldots n} \\ A^{\#} &:= \Big(\mathrm{cof}(A) \Big)^{*} \end{aligned}$$

(4.62) Example:
In case $n = 2$ the $A_{p,q}$ are particularly simple, since $A_{1,1} = a_{2,2}$ $A_{1,2} = a_{2,1}$ $A_{2,1} = a_{1,2}$ and $A_{2,2} = a_{1,1}$. Hence the cofactor matrix $\mathrm{cof}(A) = (c_{i,j})$ has the coefficients $c_{1,1} = a_{2,2}$ $c_{1,2} = -a_{2,1}$ $c_{2,1} = -a_{1,2}$ and $c_{2,2} = a_{1,1}$. To get the adjugate matrix of A all we have to do is transposing:

$$\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}^{\#} = \begin{pmatrix} a_{2,2} & -a_{1,2} \\ -a_{2,1} & a_{1,1} \end{pmatrix}$$

The next step $n = 3$ already requires some accountant's work. We will just present the result only, the reader is asked to fill in the details, as needed

$$\begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}^{\#} = \begin{pmatrix} a_{2,2}a_{3,3} - a_{2,3}a_{3,2} & a_{1,3}a_{3,2} - a_{1,2}a_{3,3} & a_{1,2}a_{2,3} - a_{1,3}a_{2,2} \\ a_{2,3}a_{3,1} - a_{2,1}a_{3,3} & a_{1,1}a_{3,3} - a_{1,3}a_{3,1} & a_{1,3}a_{2,1} - a_{1,1}a_{2,3} \\ a_{2,1}a_{3,2} - a_{2,2}a_{3,1} & a_{1,2}a_{3,1} - a_{1,1}a_{3,2} & a_{1,1}a_{2,2} - a_{1,2}a_{2,1} \end{pmatrix}$$

(4.63) Theorem: (viz. 860) **Cramer's Rule:**
Let $(R, +, \cdot)$ be any commutative ring $2 \leq n \in \mathbb{N}$ and $A \in \mathrm{mat}_n(R)$ be a $(n \times n)$-matrix over R. Then the following statements hold true

(i) For $j \in 1 \ldots n$ let us denote $a_j := \mathrm{col}_j(A)$ the j-th column-vector of A. If now $b \in R^n$ is another vector and $x = (x_1, x_2, \ldots, x_n) \in R^n$ is a solution of the SLE $Ax = b$, then for any $j \in 1 \ldots n$ the x_j satisfy the following identity

$$\det(A) x_j = \det \begin{pmatrix} | & & | & | & | & & | \\ a_1 & \cdots & a_{j-1} & b & a_{j+1} & \cdots & a_n \\ | & & | & | & | & & | \end{pmatrix}$$

(ii) The matrix A is invertible if and only if its determinant is a unit of R. And in this case the determinant of the inverse matrix is the multiplicative inverse of the determinant, that is

$$\det(A^{-1}) = \det(A)^{-1}$$

(iii) For any $A \in \mathrm{mat}_n(R)$ the adjugate matrix $A^{\#}$ of A is the same as the inverse matrix A^{-1} of A, up to the determinant $\det(A)$, as a factor. That is $A^{\#}$ satisfies the equalities below. And if $\det(A)$ (and hence A itself) is invertible we can reformulate them to get A^{-1}

$$A^{\#} A = A A^{\#} = \det(A)\, \mathbb{1}_n$$

$$A^{-1} \;=\; \det(A)^{-1}A^{\#}$$

(iv) The adjugate matrix of the transpose matrix A^* simply is the transpose of the adjugate matrix of A

$$(A^{\#})^* \;=\; (A^*)^{\#}$$

(v) If A is invertible, then so is the adjugate matrix $A^{\#}$ of A. And in this case we also give the inverse and the determinant of $A^{\#}$ to be the following

$$\begin{aligned}\left(A^{\#}\right)^{-1} &= \left(A^{-1}\right)^{\#}\\ \det\left(A^{\#}\right) &= \det(A)^{n-1}\end{aligned}$$

(4.64) Remark:
In commutative rings R, where transposition in the rule $(ab)^{-1} = b^{-1}a^{-1}$ has no impact, it is commonplace to denote the inverse of $a \in R$ by

$$\frac{1}{a} \;=\; a^{-1}$$

We usually try to avoid this, as we reserved this notation for localizations. However in this case it is worthwhile to rewrite the above equations in this notation, as it may be a little less confusing to have only one power -1. That is if $A \in \mathrm{mat}_n(R)$ is an invertible matrix, then we get

$$\begin{aligned}\det(A^{-1}) &= \frac{1}{\det(A)}\\ A^{-1} &= \frac{1}{\det(A)}A^{\#}\end{aligned}$$

(4.65) Corollary: (viz. 863)
Let $(R,+,\cdot)$ be a commutative ring, $1 \leq n \in \mathbb{N}$ and consider a square matrix $A \in \mathrm{mat}_n(R)$. Let us denote the rows of A by $r_i := \mathrm{row}_i(A)$ and the columns respectively by $c_j := \mathrm{col}_j(A)$. That is

$$A \;=\; \begin{pmatrix} \text{—} & r_1 & \text{—} \\ & \vdots & \\ \text{—} & r_n & \text{—} \end{pmatrix} \;=\; \begin{pmatrix} | & & | \\ c_1 & \cdots & c_n \\ | & & | \end{pmatrix}$$

(i) Then for any commutative ring R the following 6 statements are equivalent

(a) $\det(A) \in R^*$

(b) A is invertible

(c) $\exists\, B \in \mathrm{mat}_n(R) \;:\; AB = \mathbb{1}_n$

(d) $\exists\, B \in \mathrm{mat}_n(R) \;:\; BA = \mathbb{1}_n$

(e) $\{\, c_1, c_2, \ldots, c_n \,\}$ is a basis of R^n

(f) $\{\, r_1, r_2, \ldots, r_n \,\}$ is a basis of R^n

(ii) And for an integral domain R also the following 4 statements are equivalent

(a) $\det(A) = 0$

(b) $\mathrm{kn}(A) \neq 0$

(c) $\{ c_1, c_2, \ldots, c_n \} \subseteq R^n$ is linearly dependent

(d) $\{ r_1, r_2, \ldots, r_n \} \subseteq R^n$ is linearly dependent

(4.66) Corollary: (viz. 864) **Cramer's Rule**
Let $(R, +, \cdot)$ be any commutative ring $2 \leq n \in \mathbb{N}$ and $A = (a_{i,j}) \in \mathrm{mat}_n(R)$ be a square $(n \times n)$-matrix over R. Also let M be an R-module containing the elements $x_i \in M$ and $y_i \in M$ (where $i \in 1 \ldots n$). Finally suppose the following equations hold true

$$\begin{array}{ccccccc} a_{1,1}x_1 & + & a_{1,2}x_2 & + \cdots + & a_{1,n}x_n & = & y_1 \\ a_{2,1}x_1 & + & a_{2,2}x_2 & + \cdots + & a_{2,n}x_n & = & y_2 \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{n,1}x_1 & + & a_{n,2}x_2 & + \cdots + & a_{n,n}x_n & = & y_n \end{array}$$

Then we may compute the solution $(x_1, x_2, \ldots, x_n) \in M^n$ to the above system of linear equations in much the same way that holds true in case $M = R$. That is: For any $j \in 1 \ldots n$ we get

$$\det(A)x_j \;=\; \sum_{i=1}^{n} (-1)^{i+j} \det(A_{i,j})\, y_i$$

If A is invertible, then this is a solution formula for the x_j. And generally we thereby find the following inclusion of sub-modules of M

$$\det(A) \cdot \mathrm{Lh}\{ x_1, x_2, \ldots, x_n \} \quad \subseteq \quad \mathrm{Lh}\{ y_1, y_2, \ldots, y_n \}$$

There is a generalization to the Laplace expansion theorem that deals with determinants of whole sub-matrices of A. In the next section these determinants of sub-matrices will be called *minors* and these will play an important role for the rank of a matrix and in the theory of canonical forms. For completeness purposes we present this generalization, as well.

(4.67) Definition:
Let $1 \leq n$, $r \in \mathbb{N}$ such that $r \leq n$, then we define the set of *ascending chains of indexes* of length r by

$$\mathrm{Asc}(r, n) \;:=\; \{ \alpha : 1 \ldots r \to 1 \ldots n \mid \alpha(1) < \alpha(2) < \cdots < \alpha(r) \}$$

And if $\alpha \in \mathrm{Asc}(r, n)$ is such a chain of indexes, then we define its **scope** $S(\alpha)$ to be the set of indices that comprise α, respectively its **absolute value** $|\alpha|$ to be the sum of these indices, that is

$$\begin{aligned} S(\alpha) &:= \{ \alpha(i) \mid i \in 1 \ldots r \} \\ |\alpha| &:= \sum_{i=1}^{r} \alpha(i) \end{aligned}$$

And if $r < n$ then we also define the *complementary chain of indexes* $\widehat{\alpha} \in \mathrm{Asc}(n-r,n)$ of α to be the chain of length $n-r$ that contains exactly these numbers, that α left out. That is $\widehat{\alpha}$ is the uniquely determined ascending chain of indexes that satisfies

$$S(\widehat{\alpha}) \;=\; (1\ldots n) \setminus S(\alpha)$$

Let $(R,+,\cdot)$ be a commutative ring, $1 \leq m, n \in \mathbb{N}$ and $A \in \mathrm{mat}_{m,n}(R)$ be a matrix of any size over R. If now $1 \leq r, s \in \mathbb{N}$ and we fix the maps $\alpha : 1\ldots r \to 1\ldots m$ and $\beta : 1\ldots s \to 1\ldots n$ then we define the **sub-matrix** $A[\alpha \mid \beta]$ of A to be the following $(r \times s)$-matrix

$$A[\alpha \mid \beta] \;:=\; \begin{pmatrix} a_{\alpha(1),\beta(1)} & a_{\alpha(1),\beta(2)} & \cdots & a_{\alpha(1),\beta(s)} \\ a_{\alpha(2),\beta(1)} & a_{\alpha(2),\beta(2)} & \cdots & a_{\alpha(2),\beta(s)} \\ \vdots & \vdots & & \vdots \\ a_{\alpha(r),\beta(1)} & a_{\alpha(r),\beta(2)} & \cdots & a_{\alpha(r),\beta(s)} \end{pmatrix} \;\in\; \mathrm{mat}_{r,s}(R)$$

(4.68) Example:
We usually write out the chain of indexes $\alpha \in \mathrm{Asc}(r,n)$ as an r-tuple $(\alpha(1),\alpha(2),\ldots,\alpha(r)) \in (1\ldots n)^r$. In this notation it is clear that $\mathrm{Asc}(3,4)$ is the following set - as for any $\alpha \in \mathrm{Asc}(3,4)$ the only choice is which index to omit:

$$\mathrm{Asc}(3,4) \;=\; \{\,(1,2,3),\,(1,2,4),\,(1,3,4),\,(2,3,4)\,\}$$

Generally $\alpha \in \mathrm{Asc}(r,n)$ is uniquely determined by its scope, as we require the indices to be in ascending order. Therefore the number of elements of $\mathrm{Asc}(r,n)$ is precisely the number of subsets of $1\ldots n$ that contain r elements. This is one of the basic problems of combinatorics and the answer is

$$\#\mathrm{Asc}(r,n) \;=\; \binom{n}{r}$$

Let us also present an example of a complementary chain of indexes: If we take $\alpha = (2,5) \in \mathrm{Asc}(2,5)$ then the scope of α is $S(\alpha) = \{\,2,5\,\}$ and thereby $S(\widehat{\alpha}) = \{\,1,3,4\,\}$. That is $\widehat{\alpha} \in \mathrm{Asc}(3,5)$ has to be the chain $\widehat{\alpha} = (1,3,4)$ of indexes.

(4.69) Remark:
In the Laplace expansion theorem we used the sub-matrices $A_{p,q}$ of A. In the light of the above definition we can rewrite this as

$$A_{p,q} \;=\; A[\widehat{p} \mid \widehat{q}]$$

Thereby $\widehat{p}$ is the complementary chain of indexes of p in $1\ldots m$ and $\widehat{q}$ is the complementary chain of indexes of q in $1\ldots n$. That is $\widehat{p}$ and $\widehat{q}$ are the following maps: $\widehat{p} : 1\ldots(m-1) \to 1\ldots m$ is defined by $\widehat{p}(i) = i$ for $i < p$ and $\widehat{p}(i) = i+1$ for $i \geq p$. And likewise $\widehat{q} : 1\ldots(n-1) \to 1\ldots n$ is given to be $\widehat{q}(j) = j$ for $j < q$ and $\widehat{q}(j) = j+1$ for $j \geq q$.

(4.70) Proposition: (viz. 911)

(i) *Laplace expansion theorem:* Let $(R, +, \cdot)$ be a commutative ring and $A \in \mathrm{mat}_n(R)$ a square matrix over R. If we now fix any $r \in 1 \dots n$ and any α resp. $\beta \in \mathrm{Asc}(r, n)$, then we find

$$\begin{aligned} \det(A) &= \sum_{\beta \in \mathrm{Asc}(r,n)} (-1)^{|\alpha|+|\beta|} \det\big(A[\alpha \mid \beta]\big) \det\big(A[\widehat{\alpha} \mid \widehat{\beta}]\big) \\ &= \sum_{\alpha \in \mathrm{Asc}(r,n)} (-1)^{|\alpha|+|\beta|} \det\big(A[\alpha \mid \beta]\big) \det\big(A[\widehat{\alpha} \mid \widehat{\beta}]\big) \end{aligned}$$

(ii) *Cauchy-Binet formula:* If $(R, +, \cdot)$ is a commutative ring and A and B are matrices $A \in \mathrm{mat}_{k,m}(R)$ and $B \in \mathrm{mat}_{m,n}(R)$ such that $C := AB$ is in $C \in \mathrm{mat}_{k,n}(R)$. Then for any $r \in \mathbb{N}$ with $1 \leq r \leq \min\{ k, m, n \}$ and any $\alpha \in \mathrm{Asc}(r, k)$, $\gamma \in \mathrm{Asc}(r, n)$ we get

$$\det\big(C[\alpha \mid \gamma]\big) = \sum_{\beta \in \mathrm{Asc}(r,m)} \det\big(A[\alpha \mid \beta]\big) \det\big(B[\beta \mid \gamma]\big)$$

These formulas are truly elegant: (i) obviously is a generalization of the Laplace expansion theorem in (4.55.(v)) and (ii) generalizes the multiplicative property $\det(AB) = \det(A) \cdot \det(B)$. At the same time the Cauchy-Binet formula is astoundingly similar to the multiplication of matrices. The proofs are a different story, however: Both are technical colossi with little content from the department of insight. If you really need to look at these, you have been warned...

4.6 Rank of Matrices

In section 3.10 we have introduced the rank of a module M to be the minimal number of elements that are required to generate M. And we also found that we have to distinguish between this rank and the linear freedom, that is the maximal number of linear independent elements inside M. As the difference between these two invariants comes from torsion, they are equal when it comes to vector-spaces (i.e. when the base ring of M is a field).
For a matrix A there are even 5 different ways one can think of, when defining the rank of A. And sadly things can get rather complicated, in general. However it will turn out that that in case of an integral domain R four of these notions will have the same result. And when R is a PID (in particular for a field), all five will agree.

(4.71) Definition:
Let $(R,+,\cdot)$ be an arbitrary ring, $1 \leq m$, $n \in \mathbb{N}$ and consider a matrix $A = (a_{i,j}) \in \mathrm{mat}_{m,n}(R)$ of any size over R. Then the image of A is a sub-module $\mathrm{im}(A) \leq_{\mathsf{m}} R^m$. Thereby we define the **image-rank** of A to be the rank of the image of A, as a sub-module of R^m:

$$\text{i-rank}(A) \;:=\; \mathrm{rank}\big(\mathrm{im}(A)\big)$$

To introduce the next two notions of a rank of A we need to take a closer look at A: Let us denote the rows of A be $r_i := \mathrm{row}_i(A)$ and the columns of A by $c_j := \mathrm{col}_j(A)$, that is

$$A \;=\; \begin{pmatrix} \text{—} & r_1 & \text{—} \\ \text{—} & r_2 & \text{—} \\ & \vdots & \\ \text{—} & r_m & \text{—} \end{pmatrix} \;=\; \begin{pmatrix} | & | & & | \\ c_1 & c_2 & \dots & c_n \\ | & | & & | \end{pmatrix}$$

Then for any subset $I \subseteq 1 \dots m$ resp. any $J \subseteq 1 \dots n$ let us abbreviate the sets of rows of A with indices $i \in I$ by r_I resp. the set of columns of A with indices $j \in J$ by c_J, formally

$$\begin{aligned} r_I \;&:=\; \{\, r_i \mid i \in I \,\} \;\subseteq\; R^n \\ c_J \;&:=\; \{\, c_j \mid j \in J \,\} \;\subseteq\; R^m \end{aligned}$$

Then we define the **row-rank** (respectively the **column-rank**) of A to be the maximal number of rows (respectively columns) of A that are R-linearly independent. Formally that is

$$\begin{aligned} \text{r-rank}(A) \;&:=\; \max\left\{ \#I \;\middle|\; \begin{array}{l} I \subseteq 1 \dots m, \text{ such that} \\ r_I \text{ is } R\text{-lin. independent} \end{array} \right\} \\ \text{c-rank}(A) \;&:=\; \max\left\{ \#J \;\middle|\; \begin{array}{l} J \subseteq 1 \dots n, \text{ such that} \\ c_J \text{ is } R\text{-lin. independent} \end{array} \right\} \end{aligned}$$

(4.72) Proposition: (viz. 917)
We continue with the notation of the definition above. In the following definition M is sometimes called the *column-space* of A and N is called the *row-space* of A

$$\begin{aligned} M &:= \mathrm{Lh}\{\, c_j \mid j \in 1 \ldots m \,\} = \mathrm{im}(A) \leq_{\mathfrak{m}} R^m \\ N &:= \mathrm{Lh}\{\, r_i \mid i \in 1 \ldots n \,\} = \mathrm{im}(A^*) \leq_{\mathfrak{m}} R^n \end{aligned}$$

(i) Let $R \neq 0$ be a non-zero, commutative ring and consider any matrix $A \in \mathrm{mat}_{m,n}(R)$ over R. Then we find the following inequalities

$$\begin{aligned} \text{c-rank}(A) &\leq \text{i-rank}(A) \\ \text{c-rank}(A) &\leq \min\{\, m, n \,\} \\ \text{r-rank}(A) &\leq \min\{\, m, n \,\} \end{aligned}$$

(ii) Let $R \neq 0$ be a non-zero, commutative ring and consider two matrices $A \in \mathrm{mat}_{l,m}(R)$ and $B \in \mathrm{mat}_{m,n}(R)$ such that $AB \in \mathrm{mat}_{l,n}(R)$. Then

$$\begin{aligned} \text{c-rank}(AB) &\leq \text{c-rank}(B) \\ \text{r-rank}(AB) &\leq \text{r-rank}(A) \end{aligned}$$

In particular: If R is an integral domain, we will see in (vi) that the column- and row-ranks of A agree $\mathrm{rank}(A) := \text{c-rank}(A) = \text{r-rank}(A)$ and hence in this case we have

$$\mathrm{rank}(AB) \leq \min\{\, \mathrm{rank}(A), \mathrm{rank}(B) \,\}$$

(iii) If $1 \leq r, s \in \mathbb{N}$, $\alpha \in \mathrm{Asc}(r,m)$ and $\beta \in \mathrm{Asc}(s,n)$, then the rank of the submatrix $A[\alpha \mid \beta]$ cannot exceed the rank of A

$$\begin{aligned} \text{c-rank}(A[\alpha \mid \beta]) &\leq \text{c-rank}(A) \\ \text{r-rank}(A[\alpha \mid \beta]) &\leq \text{r-rank}(A) \end{aligned}$$

(iv) If R is an integral domain and $S \in \mathrm{mat}_m(R)$ and $T \in \mathrm{mat}_n(R)$ are square matrices with $\det(S) \neq 0$ and $\det(T) \neq 0$, then

$$\begin{aligned} \text{c-rank}(SAT) &= \text{c-rank}(A) \\ \text{r-rank}(SAT) &= \text{r-rank}(A) \end{aligned}$$

(v) If R is an integral domain and and A is in *echelon form* [recall, this means $A = 0$ or there is some $1 \leq r \in \mathbb{N}$ and some $\mu \in \mathrm{Asc}(r,n)$ such that for any $i \in 1 \ldots r$ we have $a_{i,\mu(i)} \neq 0$ but for $j < \mu(i)$ we also have $a_{i,j} = 0$. Finally $r_k = 0$ for any $k \in (r+1) \ldots m$]. Then the number of non-zero rows of A already is the column- and the row-rank of A

$$\text{c-rank}(A) = \text{r-rank}(A) = r$$

(vi) If R is an integral domain, then the column-rank of A is just the linear freedom of the image of A and hence does not exceed the image rank of A. Also the row-rank of A is just the linear freedom of N and agrees with the column-rank of A. That is

$$\begin{aligned} \text{c-rank}(A) &= \text{free}\big(M\big) \leq \text{i-rank}(A) \\ \text{r-rank}(A) &= \text{free}\big(N\big) = \text{c-rank}(A) \end{aligned}$$

(vii) If R is a PID (in particular an integral domain), then the rank of the image $\text{im}(A)$ equals the column-rank of A and hence we have the following (in)equalties

$$\text{c-rank}(A) = \text{r-rank}(A) = \text{i-rank}(A) \leq \min\{\, m, n \,\}$$

(viii) If R is a skew-field, then the row-rank of A is precisely the dimension of N (as a vector-space). Likewise the column-rank of A is the dimension of M and both agree. These are the equalities of

$$\text{i-rank}(A) = \text{c-rank}(A) = \dim(M) = \dim(N) = \text{r-rank}(A)$$

(ix) Let R be an integral domain again and $x_1, x_2, \ldots, x_m \in R^n$ be n-tuples where $1 \leq m \leq n \in \mathbb{N}$ where $1 \leq m \leq n \in \mathbb{N}$. For $\alpha \in \text{Asc}(m,n)$ let us also denote the projection $P_\alpha : R^n \to R^m$ that is defined by $P_\alpha(a_1, \ldots, a_n) = (a_{\alpha(1)}, \ldots, a_{\alpha(m)})$. Then we find the following equivalence [for a general commutative ring R we still have (b) $\implies$ (a)]

(a) $\{\, x_1, \ldots, x_m \,\} \subseteq R^n$ is linearly independent

(b) There is some $\alpha \in \text{Asc}(m,n)$ such that the set of projected n-tuples $\{\, P_\alpha(x_1), \ldots, P_\alpha(x_m) \,\} \subseteq R^m$ is linearly independent.

(4.73) Remark:
The tricky part in this proof is to show that the row-rank matches the column rank $\text{c-rank}(A) = \text{r-rank}(A)$. Most textbooks derive this result from (iv) and (v): If we had (iv) and (v) then we could use Gaussian elimination (4.29) to find some matrix $S \in \text{mat}_n(R)$ such that SA is in echelon form. Thereby S can be taken to be a product of elementary matrices. And as any elementary matrix has non-zero determinant, so does S. Then we see

$$\text{c-rank}(A) = \text{c-rank}(SA) = \text{r-rank}(SA) = \text{r-rank}(A)$$

We will derive (iv) from the equality however. Another method is using the minorial rank $\text{m-rank}(A)$, which we will introduce next. It is clear that $\text{m-rank}(A) = \text{m-rank}(A^*)$, as the determinants are invariant under transposition. So if we are able to prove $\text{c-rank}(A) = \text{m-rank}(A)$ then we clearly have $\text{r-rank}(A) = \text{c-rank}(A^*) = \text{m-rank}(A^*) = \text{m-rank}(A) = \text{c-rank}(A)$, as well. In fact we will also give prove for $\text{c-rank}(A) = \text{m-rank}(A)$, but wanted to give an independent proof of $\text{c-rank}(A) = \text{r-rank}(A)$ beforehand, even though this requires the somewhat advanced lemma (3.99.(i)).

(4.74) Example:
If R is *not* an integral domain, then a matrix in echelon form may well have fewer (column) rank, then its size suggests. Also in this case row-rank and column-rank need no longer agree. Over $R = \mathbb{Z}_6$ for example, we take a look at the following (3×4)-matrix

$$A := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix} \in \mathrm{mat}_{3,4}(\mathbb{Z}_6)$$

This matrix features $1 = \text{c-rank}(A) < \text{r-rank}(A) = 2 < 3$. Prob First of all it is clear that $\{ c_1 \}$ is linearly independent, but as $2c_2 = 0$, $3c_2 = 0$ and also $2c_4 = 0$ this set can not be extended, such that $\text{c-rank}(A) = 1$. Also $\{ r_1, r_2 \}$ is linearly independent: suppose $0 = ar_1 + br_2 = (a, 3b, 2b, 0)$, then $a = 0$ is obvious. But $3b = 0$ only leaves $b \in \{ 0, 2, 4 \}$ and $2b = 0$ only leaves $b \in \{ 0, 3 \}$. Since b is this same we also get $b = 0$. But as $2r_3 = 0$ as well, neither $\{ r_1, r_2 \}$ can be extended. Therefore $\text{r-rank}(A) = 2$, as claimed.

(4.75) Example:
If R is *not* an integral domain, then the image-rank of A may well exceed the column-rank of A. As an example take the ring $R := \mathbb{Z}_{70}$ and consider the matrix

$$A := \begin{pmatrix} 3 & 10 \\ 3 & 14 \end{pmatrix}$$

having the column vectors $c_1 = (3, 3)$ and $c_2 = (10, 14)$. As $3 \in R^*$ (with inverse 47) clearly $\{ c_1 \}$ is linearly independent. However $35c_2 = (0, 0)$ such that $\{ c_2 \}$ is linearly dependent. Therefore $\text{c-rank}(A) = 1$ with c_1 being the one linearly independent column. Yet $c_2 \notin Rc_1$ such that $\mathrm{im}(A)$ cannot be generated by a single element, as $\mathrm{im}(A)$ contains both $(1, 1)$ and $(20, 0)$. Therefore $2 = \text{i-rank}(A) \geq \text{c-rank}(A) = 1$.

(4.76) Example:
But even if R *is* an integral domain the image-rank of a matrix A may exceed its column-rank (or any rank equal to it). A very easy, but instructive example is the following: Let $R := \mathbb{Z}[t]$ be the polynomial ring over the integers and consider

$$A := \begin{pmatrix} 2 & t \end{pmatrix} \in \mathrm{mat}_{1,2}(R)$$

Its image clearly is $2R + tR = \{ f \in R \mid f[0] \in 2\mathbb{Z} \}$. As this image cannot be generated by a single $g \in R$ we have $\text{i-rank}(A) = 2$. Yet the column rank cannot exceed 1 and hence $\text{c-rank}(A) < \text{i-rank}(A)$.

(4.77) Example:
If R is a PID, then the image-rank and column-rank of A agree. However this is *not* due to the fact, that a maximal linearly independent subset of columns suffices to build up the image of A. E.g. regard

$$A := \begin{pmatrix} 2 & 0 & 4 \\ 0 & 3 & 4 \end{pmatrix}$$

Clearly the columns $(2,0)$ and $(0,3)$ are linearly independent and hence c-rank$(A) = 2$. They generate the sub-module $2\mathbb{Z} \oplus 3\mathbb{Z}$ of $\mathbb{Z}^2$. Yet this image of A also is generated by $(4,4) \notin 2\mathbb{Z} \oplus 3\mathbb{Z}$ and therefore

$$\mathsf{Lh}\left\{ \begin{pmatrix} 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \end{pmatrix} \right\} \;=\; 2\mathbb{Z} \oplus 3\mathbb{Z} \quad\subset\quad \mathsf{im}(A) \;=\; 2\mathbb{Z} \oplus \mathbb{Z} \quad\subset\quad \mathbb{Z}^2$$

(4.78) Remark:
The equality of the row- and the column-rank of matrices over an integral domain R is a *really* strong property though. This can be gleaned from item (ix), which is a direct consequence of this equality. Generally speaking (ix) states: Over an integral domain R the linear dependency of the tuples x_1, $x_2, \ldots, x_m \in R^n$ is determined in m dimensions already, no matter how many $n \geq m$ entries these tuples have. And if R is not an integral domain, this property vanishes: As an example consider the ring $R = \mathbb{Z}_{30}$ and the following matrix

$$A \;=\; \begin{pmatrix} 6 & 4 \\ 9 & 6 \\ 7 & 5 \end{pmatrix} \;\in\; \mathsf{mat}_{3,2}(R)$$

First of all we note that c-rank$(A) = 2$: Suppose we had $aA_1 + bA_2 = 0$ then this would mean the equations $6a + 4b = 0$ and $9a + 6b = 0$ and $7a + 5b = 0$. Subtracting the first from the third equation we find $a + b = 0$. But equation one then turns into $2a = 0$ and equation two into $3a = 0$. This again means $a = 0$ and in turn $b = 0$, such that we see that A_1 and A_2 are linearly independent. However all the (2×2)-sub-matrices of A have column-rank 1 only, as we can easily present some linear dependencies

$$\begin{aligned} 10 \begin{pmatrix} 6 \\ 9 \end{pmatrix} + 0 \begin{pmatrix} 4 \\ 6 \end{pmatrix} &= \begin{pmatrix} 0 \\ 0 \end{pmatrix} \\ 15 \begin{pmatrix} 6 \\ 7 \end{pmatrix} + 15 \begin{pmatrix} 4 \\ 5 \end{pmatrix} &= \begin{pmatrix} 0 \\ 0 \end{pmatrix} \\ 10 \begin{pmatrix} 9 \\ 7 \end{pmatrix} + 10 \begin{pmatrix} 6 \\ 5 \end{pmatrix} &= \begin{pmatrix} 0 \\ 0 \end{pmatrix} \end{aligned}$$

(4.79) Proposition: (viz. 925)
If $(F, +, \cdot)$ is a field and $A \in \mathsf{mat}_{m,n}(F)$ is a matrix over F, where $1 \leq m$, $n \in \mathbb{N}$. Let us abbreviate $r_i := \mathsf{row}_i(A) \in F^n$ and $c_j := \mathsf{col}_j(A)$ for any $i \in 1 \ldots m$ and $j \in \ldots n$. Now consider any $r \in \mathbb{N}$, then the following five statements are equivalent

(a) c-rank$(A) \;\leq\; r$

(b) A has r columns, that generate all of its columns. I.e. there is some subset $J \subseteq 1 \ldots n$ with $\#J = r$ such that for any $k \in 1 \ldots n$ we have

$$c_k \;\in\; \mathsf{Lh}_F\{\, c_j \mid j \in J \,\}$$

(c) There are matrices $C \in \mathrm{mat}_{m,r}(F)$ and $R \in \mathrm{mat}_{r,n}(F)$ such that A can be factored into a product of the following form

$$A \;=\; C\,R$$

(d) A has r rows, that generate all of its rows. I.e. there is some subset $I \subseteq 1 \ldots m$ with $\#I = r$ such that for any $k \in 1 \ldots m$ we have

$$r_k \;\in\; \mathrm{Lh}_F\{\, r_j \mid j \in J \,\}$$

(e) $\text{r-rank}(A) \;\leq\; r$

In particular - for a field F - the column-rank (or likewise row-rank) of A can be characterized as the minimal number r for which A admits a decomposition of the form $A = CR$:

$$\text{c-rank}(A) \;=\; \text{r-rank}(A) \;=\; \min\{\, r \in \mathbb{N} \mid \;\; \text{(c)} \,\}$$

(4.80) Remark:
Note that this provides a rather elegant method of proving $\text{c-rank}(A) = \text{r-rank}(A)$ in case the base ring is a field. The only non-elementary ingredients in the proof are the basis selection theorem and (ii) the sub-multiplicativety of the rank $\text{c-rank}(CR) \leq \text{c-rank}(R)$ and $\text{r-rank}(CR) \leq \text{r-rank}(C)$. But the latter property is easy to see, as well.

(4.81) Definition:
Let $(R, +, \cdot)$ be a commutative ring, $1 \leq m$, $n \in \mathbb{N}$ and consider a matrix $A \in \mathrm{mat}_{m,n}(R)$ of any size over R. If furthermore $r \in 1 \ldots \min\{\, m, n \,\}$ and $\alpha \in \mathrm{Asc}(r, m)$, $\beta \in \mathrm{Asc}(r, n)$ are ascending chains of indexes then recall the notation of a *submatrix*

$$A[\alpha \mid \beta] \;=\; \begin{pmatrix} a_{\alpha(1),\beta(1)} & a_{\alpha(1),\beta(2)} & \cdots & a_{\alpha(1),\beta(r)} \\ a_{\alpha(2),\beta(1)} & a_{\alpha(2),\beta(2)} & \cdots & a_{\alpha(2),\beta(r)} \\ \vdots & \vdots & & \vdots \\ a_{\alpha(r),\beta(1)} & a_{\alpha(r),\beta(2)} & \cdots & a_{\alpha(r),\beta(r)} \end{pmatrix} \;\in\; \mathrm{mat}_r(R)$$

The determinant of such a submatrix of A is called a **minor** of **size** r or simply r-**minor** of A. We will denote the set of all r-minors of A by

$$\mathrm{Minor}_r(A) \;:=\; \{\, \det(A[\alpha \mid \beta]) \;\mid\; \alpha \in \mathrm{Asc}(r, m),\, \beta \in \mathrm{Asc}(r, n) \,\} \;\subseteq\; R$$

The **minorial rank** (also called **determinantal rank**) of A is the largest integer such that not all r-minors of A vanish [if $A = 0$ is the zero-matrix this set is empty and we let $\text{m-rank}(0) := 0$]

$$\text{m-rank}(A) \;:=\; \max\{\, r \in 1 \ldots \min\{\, m, n \,\} \mid \mathrm{Minor}_r(A) \neq \{0\} \,\}$$

Now for any $1 \leq r \leq \min\{ m, n \}$ the ideal generated by the set of r-minors of A is said to be the r-th **Fitting ideal** of A, which we will denote by

$$\mathfrak{f}_r(A) \;:=\; \langle \mathrm{Minor}_r(A) \rangle_{\mathrm{i}} \;\trianglelefteq_{\mathrm{i}}\; R$$

For completeness purposes we also define $\mathfrak{f}_0(A) := R$ and for any larger index $\min\{ m, n \} < r \in \mathbb{N}$ we let $\mathfrak{f}_r(A) := 0 \trianglelefteq_{\mathrm{i}} R$. If R is a PID, then any ideal of R is generated by a single element $\mathfrak{f}_r(A) = d_r R$. In this case a generator $d_r \in R$ of $\mathfrak{f}_r(A)$ is called an r-th **determinantal divisor** of A. Finally we define the **Fitting rank** of A to be the largest integer r such that the annihilator ideal of $\mathfrak{f}_r(A)$ vanishes

$$\text{f-rank}(A) \;:=\; \max\{ r \in \mathbb{N} \mid \mathrm{ann}\,(\mathfrak{f}_r(A)) = 0 \}$$

(4.82) Example:
Let us give some examples of sets of minors of an arbitrary matrix $A = (a_{i,j}) \in \mathrm{mat}_{m,n}(R)$ over some commutative ring R. Clearly we have

$$\begin{aligned} \mathrm{Minor}_1(A) &= \left\{ a_{i,j} \;\middle|\; \begin{array}{l} i \in 1 \ldots m, \\ j \in 1 \ldots n \end{array} \right\} \\ \mathrm{Minor}_2(A) &= \left\{ a_{p,q}a_{r,s} - a_{r,q}a_{p,s} \;\middle|\; \begin{array}{l} 1 \leq p < r \leq m, \\ 1 \leq r < s \leq n \end{array} \right\} \end{aligned}$$

And if $A \in \mathrm{mat}_n(R)$ is a square matrix over R, then it is clear that A is the only $n \times n$ submatrix of itself

$$A \text{ square matrix} \;\Longrightarrow\; \mathrm{Minor}_n(A) \;=\; \{ \det(A) \}$$

(4.83) Proposition: (viz. 926)
Let $(R, +, \cdot)$ be a commutative ring and consider a matrix $A \in \mathrm{mat}_{m,n}(R)$ where $1 \leq m, n \in \mathbb{N}$ over R. Given $r, s \in \mathbb{N}$ with $1 \leq r, s \leq \min\{ m, n \}$ fix some $\alpha \in \mathrm{Asc}(r, m)$ and $\beta \in \mathrm{Asc}(s, n)$. Then we find:

(i) We have $A[\alpha \mid \beta]^* = A^*[\beta \mid \alpha]$ and in particular the matrix A and its transpose A^* share the same minors. Formally this is the identity of the sets

$$\mathrm{Minor}_r(A) \;=\; \mathrm{Minor}_r(A^*)$$

Consequentially we have the equalities $\mathfrak{f}_r(A^*) = \mathfrak{f}_r(A)$ and thereby $\text{f-rank}(A^*) = \text{f-rank}(A)$ and of course $\text{m-rank}(A^*) = \text{m-rank}(A)$.

(ii) For any $1 \leq r \leq m, n$ the r-minors are invariant under elementary equivalence up to sign. That is: If we denote $\pm M := \{ m \mid m \in M \} \cup \{ -m \mid m \in M \}$ for any subset $M \subseteq R$, then

$$A \equiv B \;\Longrightarrow\; \pm\mathrm{Minor}_r A = \pm\mathrm{Minor}_r B$$

(iii) By the Laplace expansion theorem the r-minors of A are R-linear combinations of the $(r-1)$-minors of A. In particular we find the following inclusions

$$\mathrm{Minor}_r(A) \;\subseteq\; \mathfrak{f}_{r-1}(A)$$

$$\mathfrak{f}_r(A) \;\subseteq\; \mathfrak{f}_1(A)^r$$

$$\mathrm{Minor}_{r-1}(A) \;=\; \{0\} \quad\Longrightarrow\quad \mathrm{Minor}_r(A) \;=\; \{0\}$$

And thereby the fitting ideals of A form a descending chain of ideals in R. Also, if we denote $\mu := \min\{\, m, n \,\}$, then by definition of these ideals we know that this chain has the form

$$R \;=\; \mathfrak{f}_0(A) \;\supseteq\; \mathfrak{f}_1(A) \;\supseteq\; \ldots \;\supseteq\; \mathfrak{f}_\mu(A) \;\supseteq\; \mathfrak{f}_{\mu+1}(A) \;=\; \ldots \;=\; 0$$

(iv) By definition the annihilator of a Fitting ideal of A is the set of all $a \in R$ that make $am = 0$ for any $m \in \mathfrak{f}_r(A)$. But as the minors $\mathrm{Minor}_r(A)$ generate that ideal, it is clear that

$$\mathrm{ann}\,(\mathfrak{f}_r(A)) \;=\; \{\, a \in R \;\mid\; \forall\, m \in \mathrm{Minor}_r(A) \,:\, am = 0 \,\}$$

And since the Fitting ideals form a descending chain of ideals, their annihilators form an ascending chain. With $\mu := \min\{\, m, n \,\}$ again this is the following chain of ideals

$$0 = \mathrm{ann}(\mathfrak{f}_0(A)) \;\subseteq\; \ldots \;\subseteq\; \mathrm{ann}(\mathfrak{f}_\mu(A)) \;\subseteq\; \mathrm{ann}(\mathfrak{f}_{\mu+1}(A)) = \cdots = R$$

(v) If $A' = A[\alpha \mid \beta]$ is a submatrix of A, then its minorial rank and its fitting rank do not exceed the respective rank of A, that is we find the following inequalities

$$\begin{aligned} \text{m-rank}(A') \;&\leq\; \text{m-rank}(A) \\ \text{f-rank}(A') \;&\leq\; \text{f-rank}(A) \end{aligned}$$

(vi) If A has a minor $m \in \mathrm{Minor}_r(A)$ with trivial annihilator only, then the column- and row-ranks of A are at least r, formally this is

$$\mathrm{ann}\,(\det\,(A[\alpha \mid \beta])) = 0 \quad\Longrightarrow\quad \min\{\, \text{c-rank}(A), \text{r-rank}(A) \,\} \geq r$$

(vii) The minorial rank is submultiplicative, that is: If $A \in \mathrm{mat}_{k,m}(R)$ and $B \in \mathrm{mat}_{m,n}(R)$ for some $1 \leq k$, m and $n \in \mathbb{N}$, then we have

$$\text{m-rank}(AB) \;\leq\; \min\{\, \text{m-rank}(A), \text{m-rank}(B) \,\}$$

(viii) The matrix A (as a linear map $R^n \to R^m$) has no kernel if and only if its column-rank is n which is again equivalent to a Fitting-rank of n. Altogether

$$\mathrm{kn}(A) = 0 \;\Longleftrightarrow\; \text{c-rank}(A) = n \;\Longleftrightarrow\; \text{f-rank}(A) = n$$

(4.84) Example:
Consider any commutative ring $(R,+,\cdot)$, $1 \leq m,n \in \mathbb{N}$ and a pair of tuples $u = (u_1,u_2,\ldots,u_m) \in R^m$ and $v = (v_1,v_2,\ldots,v_n) \in R^n$. If now $A \in \mathrm{mat}_{m,n}(R)$ is the following matrix

$$A \;=\; \big(u_i v_j\big) \;=\; \begin{pmatrix} u_1v_1 & u_1v_2 & \ldots & u_1v_n \\ u_2v_1 & u_2v_2 & \ldots & u_2v_n \\ \vdots & \vdots & & \vdots \\ u_mv_n & u_mv_2 & \ldots & u_mv_n \end{pmatrix}$$

Then for any $x = (x_1,x_2,\ldots,x_n) \in R^n$ we get $Ax = \langle x \mid v\rangle\, u \in R^m$ [if R is non-commutative, then $Ax = u\,\langle v \mid x\rangle$ still]. And thereby we have

$$\text{c-rank}(A) \;=\; \text{r-rank}(A) \;=\; \text{m-rank}(A) \;\leq\; 1$$

Prob If $A = 0$ then all these ranks are 0, so let us assume $A \neq 0$. Next note that $\mathrm{col}_j(A) = v_j u$ such that any two columns of A are linearly dependent $v_i\mathrm{col}_j(A) - v_j\mathrm{col}_i(A) = 0$. Therefore c-rank$(A) \leq 1$, which only leaves c-rank$(A) = 1$, since $A \neq 0$. Likewise r-rank$(A) = 1$, as we also have $\mathrm{row}_i(A) = u_i v$. The minorial rank of A also is m-rank$(A) \leq 1$, e.g. $\det(A[(1,2) \mid (1,2)] = u_1v_1u_2v_2 - u_1v_2u_2v_1 = 0$, since R is commutative. The same is true for all the 2×2 minors of A. And as $A \neq 0$ this is m-rank$(A) = 1$, as well.

(4.85) Remark:
Given 2 vectors $x = (x_1,x_2,x_3)$ and $y = (y_1,y_2,y_3)$ in 3 dimensional space R^3 it stands to reason that there is precisely one direction perpendicular to both x and y. As we will see in chapter 4.8 the orthogonality $x \perp n$ and $y \perp n$ (for some $n = (n_1,n_2,n_3) \in R^3$) can be expressed in the equation

$$\begin{pmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \end{pmatrix} \begin{pmatrix} n_1 \\ n_2 \\ n_3 \end{pmatrix} \;=\; \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

By Cramer's rule a solution n to this set of equations can be given in terms of the 2-minors of the matrix above and this is the so-called *vector-product* of x and y

$$n \;=\; x \wedge y \;:=\; \begin{pmatrix} x_2y_3 - x_3y_2 \\ x_3y_1 - x_1y_3 \\ x_1y_2 - x_2y_1 \end{pmatrix}$$

If R is an integral domain and x and y are linearly independent, then $x \wedge y \neq 0$ since f-rank$(A) =$ r-rank$(A) = 2$. If R is no integral domain, then it may happen, that $x \wedge y = 0$ even if x and y are linearly independent (refer to the example above). This is hard to imagine: The projections of x and y on any coordinate plane are in line, even though in space x and y themselves are not.

(4.86) Theorem: (viz. 932)
Let $(R,+,\cdot)$ be a commutative ring, $1 \leq m,n \in \mathbb{N}$ and $A \in \mathrm{mat}_{m,n}(R)$ be a matrix over R of any size. Then the column- and row-ranks do not exceed the Fitting rank, which in turn is bound by the minorial rank. That is we generally have the inequalities

$$\max\{\,\text{c-rank}(A), \text{r-rank}(A)\,\} \;\leq\; \text{f-rank}(A) \;\leq\; \text{m-rank}(A) \;\leq\; \min\{\,m,n\,\}$$

If R even is an integral domain, then the row-, column-, fitting- and minorial ranks of a matrix always agree. That is in this case we even get the equalities

$$\text{c-rank}(A) \;=\; \text{r-rank}(A) \;=\; \text{f-rank}(A) \;=\; \text{m-rank}(A)$$

And finally, if R is a field, then all five notions of the rank of a matrix yield the same result, that is

$$\text{i-rank}(A) \;=\; \text{c-rank}(A) \;=\; \text{r-rank}(A) \;=\; \text{f-rank}(A) \;=\; \text{m-rank}(A)$$

(4.87) Example:
The following ingenious example is taken from [Adkins, Weintraub, Algebra, GTM 136], who sadly (while stating most theorems of this section) give next to no proof at all, concerning the rank of matrices. Consider the ring $R = \mathbb{Z}_{210}$ and the following (4×4)-matrix over R:

$$A \;:=\; \begin{pmatrix} 0 & 2 & 3 & 5 \\ 2 & 0 & 6 & 0 \\ 3 & 0 & 3 & 0 \\ 0 & 0 & 0 & 7 \end{pmatrix}$$

This matrix boasts four different ranks! We will find, that A has the following ranks of the resp. kind

$$\begin{aligned} \text{r-rank}(A) &= 1 \\ \text{c-rank}(A) &= 2 \\ \text{f-rank}(A) &= 3 \\ \text{m-rank}(A) &= 4 \\ \text{i-rank}(A) &= 4 \end{aligned}$$

Let us first check the row rank, as $105\,\mathrm{row}_2(A) = 0$ and $70\,\mathrm{row}_3(A) = 0$ but also $30\,\mathrm{row}_4(A) = 0$ we only have to look at the first row. But here, if $a\,\mathrm{row}_1(A) = 0$, we in particular find $2a = 0$ and $3a = 0$, such that $a = 3a - 2a = 0$. Therefore we have r-rank$(A) = 1$, as the first is the one and only linearly independent row.
For the column rank we likewise find $105\,\mathrm{col}_2(A) = 0$ and $70\,\mathrm{col}_3(A) = 0$. But hereby, if we have $a\,\mathrm{col}_1(A) + b\,\mathrm{col}_4(A) = 0$ we have $2a = 0$, $3a = 0$ and $5b = 0$, $7b = 0$. From the first set of equations we find $a = 0$, as before. From the second set we get $b \in \mathrm{ann}(5) \cap \mathrm{ann}(7) = 42R \cap 30R$. But as the least common multiple of 30 and 42 is $210 = 0$ this implies $b \in 210R = 0$. Therefore the first and fourth columns are linearly independent and we truly have c-rank$(A) = 2$.

Actually the easiest part is the determinantal rank, since $\det(A) = 168 \neq 0$ we have m-rank$(A) = 4$. But as $5 \cdot 168 = 840 = 0$ we have $\operatorname{ann}(\det(A)) \neq 0$ such that f-rank$(A) \leq 3$. To find the equality let us take a look at the 16 (3×3)-minors of A:

submatrix	minor = det	annihilator
$A_{1,1}$	0	R
$A_{1,2}$	$-84 = 126$	$105R$
$A_{1,3}$	0	R
$A_{1,4}$	0	R
$A_{2,1}$	42	$5R$
$A_{2,2}$	$-63 = 147$	$10R$
$A_{2,3}$	$-42 = 168$	$5R$
$A_{2,4}$	0	R
$A_{3,1}$	84	$5R$
$A_{3,2}$	$-42 = 168$	$5R$
$A_{3,3}$	$-28 = 182$	$15R$
$A_{3,4}$	0	R
$A_{4,1}$	0	R
$A_{4,2}$	$-60 = 150$	$7R$
$A_{4,3}$	0	R
$A_{4,4}$	24	$35R$

Note that $\{ 24, 147, 182 \} \subseteq \operatorname{Minor}_3(A)$. And from this we find $\mathfrak{f}_3(A) = R$, for example we have $1 = 7 \cdot 147 + 2 \cdot 182 - 58 \cdot 24 \in \mathfrak{f}_3(A)$ and therefore $\operatorname{ann}(\mathfrak{f}_3(A)) = 0$, such that m-rank$(A) = 3$.
Recall that these minors are precisely the coefficients of the cofactor matrix of A and therefore we can also build up the adjugate matrix of A. In this case we get

$$A^{\#} = \begin{pmatrix} 0 & -42 & 84 & 0 \\ 84 & -63 & 42 & -60 \\ 0 & 42 & -28 & 0 \\ 0 & 0 & 0 & 24 \end{pmatrix} = \begin{pmatrix} 0 & 168 & 84 & 0 \\ 84 & 147 & 42 & 150 \\ 0 & 42 & 182 & 0 \\ 0 & 0 & 0 & 24 \end{pmatrix}$$

As $AA^{\#}x = \det(A)x = 168x$ for any $x \in R^4$ we see, that the image of A contains the vectors $(168, 0, 0, 0)$ to $(0, 0, 0, 168)$. But these cannot be generated by three vectors and hence A has i-rank$(A) = 4$.

(4.88) Lemma: (viz. 934)
Smith normal Form: Let (R,v) be an Euclidean domain, $1 \leq m$, $n \in \mathbb{N}$ and $A \in \mathrm{mat}_{m,n}(R)$ be any matrix over R. Then we find the truth of the following statements

(i) If $m \leq n$ then we can find scalar factors $d_1,\ldots,d_m \in R$ that form a divisibly ascending chain, i.e. $d_1 \mid d_2,\ldots,d_{m-1} \mid d_m$ such that A is elementary equivalent to

$$A \equiv \begin{pmatrix} d_1 & & 0 & 0 & \ldots & 0 \\ & \ddots & & \vdots & & \vdots \\ 0 & & d_m & 0 & \ldots & 0 \end{pmatrix}$$

And for any $r \in 1\ldots m$ we find that the scalar factors $d_1,\ldots,d_m$ can be expressed in terms of minors of A: The product $d_1 \ldots d_r$ is a greatest common divisor of the r-minors of A. In particular the d_i are uniquely determined by A up to multiplication with units of R. Formally

$$d_1 \ldots d_r \quad \in \quad \gcd(\mathrm{Minor}_r A)$$

(ii) If $n \leq m$ then we can find scalar factors $d_1,\ldots,d_n \in R$ that form a divisibly ascending chain, i.e. $d_1 \mid d_2,\ldots,d_{n-1} \mid d_n$ such that A is elementary equivalent to

$$A \equiv \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \\ 0 & \ldots & 0 \\ \vdots & & \vdots \\ 0 & \ldots & 0 \end{pmatrix}$$

And for any $r \in 1\ldots m$ we find that the scalar factors $d_1,\ldots,d_n$ can be expressed in terms of minors of A: The product $d_1 \ldots d_r$ is a greatest common divisor of the r-minors of A. In particular the d_j are uniquely determined by A up to multiplication with units of R. Formally

$$d_1 \ldots d_r \quad \in \quad \gcd(\mathrm{Minor}_r A)$$

4.7 Duality Theory

In R^n we have introduced the scalar product $\langle x, y\rangle$ of two tuples x, $y \in R^n$. Let us look at this from another perspective: For any $y \in R^n$ the scalar product gives rise to a linear map, of the form

$$R^n \to R \ : \ x \mapsto \langle x, y\rangle$$

The set of all linear maps of the form $M \to R$ will be called the *dual module* M' of M. So the scalar product induces a map from R^n to $(R^n)'$. In this section we will study the relation between M and its dual M' and see that this is closely linked to studying bilinear forms - such as the scalar product.
This is extremely fruitful in the case of the base field $\mathbb{R}$ or $\mathbb{C}$ and is the staging point of a lot of important theories - like Fourier analysis and Hilbert space theory in general. So at several points throughout this section we will have to leave the all-encompassing domain of modules and have to restrict ourselves to vector spaces over the reals or complex numbers.

(4.89) Remark:
Recall the construction of the complex numbers $\mathbb{C} = \mathbb{R} \oplus i\mathbb{R}$ in (1.35.(i)). Thereby we have several maps

$$\begin{aligned} \mathrm{re} &: \mathbb{C} \to \mathbb{R} : \ x + iy \mapsto x \\ \mathrm{im} &: \mathbb{C} \to \mathbb{R} : \ x + iy \mapsto y \\ \kappa &: \mathbb{C} \to \mathbb{C} : \ x + iy \mapsto x - iy \end{aligned}$$

The map κ is called the **complex conjugation** and we write $\overline{z} := \kappa(z)$. Note that κ is an automorphism of the $\mathbb{R}$-algebra $\mathbb{C}$. That is for any w, $z \in \mathbb{C}$ and any $a \in \mathbb{R}$ we get

$$\begin{aligned} \overline{w+z} &= \overline{w} + \overline{z} \\ \overline{a \cdot z} &= a \cdot \overline{z} \\ \overline{w \cdot z} &= \overline{w} \cdot \overline{z} \end{aligned}$$

Also note that re and im are $\mathbb{R}$-linear only and do *not* respect the multiplication of $\mathbb{C}$. It is clear that κ is self-inverse $\kappa^2 = \mathbb{1}_{\mathbb{C}}$ and satisfies a special property: For any $z = x + iy$ we find

$$z \cdot \overline{z} \ = \ x^2 + y^2 \ \in \ \mathbb{R}^+$$

In particular we may define the **absolute value** $|z|$ of $z = x + iy \in \mathbb{C}$ which we interpret as the the distance of z from the origin 0

$$|z| \ := \ \sqrt{z \cdot \overline{z}} \ = \ \sqrt{x^2 + y^2}$$

Recall that the complex conjugation and absolute value of a complex number $z \in \mathbb{C}$ with $z \neq 0$ also provide a way to find the inverse of z

$$z^{-1} \ = \ \frac{1}{|z|^2}\overline{z} \ = \ \frac{x - iy}{x^2 + y^2}$$

In the next section 4.8 we will introduce sine and cosine [even though the reader will probably know these already] and see that any point $(x,y) = x + iy$ in the plane $\mathbb{R}^2 = \mathbb{C}$ can be reached by by virtue of the **polar coordinates**

$$\mathbb{R}^+ \times [0, 2\pi[\to \mathbb{C} \ : \ (r,\alpha) \mapsto r \cdot \cos(\alpha) + ir \cdot \sin(\alpha)$$

If we take $\mathbb{R}_{>0} \times [0, 2\pi[\to \mathbb{C}^*$ this map even is bijective, its inverse given by $z \mapsto (|z|, \arg(z))$, where the angle $\alpha = \arg(z)$ of z can be computed by painstakingly distinguishing all the different cases, in what quadrant z is

$$\arg(z) \quad = \quad \begin{cases} 0 & \text{if } x = 0 \text{ and } y = 0 \\ \tan^{-1}(y/x) & \text{if } x > 0 \text{ and } y \geq 0 \\ \pi/2 & \text{if } x = 0 \text{ and } y > 0 \\ \pi/2 - \tan^{-1}(x/y) & \text{if } x < 0 \text{ and } y > 0 \\ \pi + \tan^{-1}(y/x) & \text{if } x < 0 \text{ and } y \leq 0 \\ 3\pi/2 & \text{if } x = 0 \text{ and } y < 0 \\ 2\pi + \tan^{-1}(y/x) & \text{if } x > 0 \text{ and } y < 0 \end{cases}$$

Another way to use polar coordinates in the famous formula of Euler (■) which links the exponential function with sine and cosine in the following way

$$r \cdot e^{i\alpha} \quad = \quad r \cdot \cos(\alpha) + ir \cdot \sin(\alpha)$$

That is $z = |z| \cdot e^{i \cdot \arg(z)}$ for any $z \in \mathbb{C}$. The formula of Euler is usually proved in a course of analysis by comparing the power series expansions of the exponential function, sine and cosine respectively. It can be seen that sine gets the odd exponents and cosine gets the even exponents of the exponential series. However, we don't want to go into details here.

$$\begin{aligned} e^z &= \sum_{k=0}^{\infty} \frac{1}{k!} z^k \\ \sin(z) &= \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k+1)!} z^{2k+1} \\ \cos(z) &= \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k)!} z^{2k} \end{aligned}$$

The representation in polar coordinates has the advantage that $z \mapsto e^z$ is a homomorphism from the additive group $(\mathbb{C}, +)$ to the multiplicative group $(\mathbb{C}^*, \cdot)$. That is we have the following formula

$$\begin{aligned} e^0 &= 1 \\ e^{w+z} &= e^w \cdot e^z \end{aligned}$$

for any $w, z \in \mathbb{C}$. In the case of the reals this even is an isomorphism of from $(\mathbb{R}, +)$ to $(\mathbb{R}_{>0}, \cdot)$ but in the complex case things are a little more complex. However the homorphism property yields

$$\left(r \cdot e^{i\alpha}\right) \cdot \left(s \cdot e^{i\beta}\right) \quad = \quad rs \cdot e^{i(\alpha+\beta)}$$

(4.90) Remark:
For any commutative ring $(R,+,\cdot)$ and any $1 \leq n \in \mathbb{N}$ we introduced the **scalar product** to be the following symmetric bilinear form on R^n

$$R^n \times R^n \ :\to \ R \ : \ (x,y) \ \mapsto \ \langle x,y\rangle \ := \ \sum_{i=1}^{n} x_i y_i$$

where $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$. This notation hides the dimension n however, so in fact theses are infinitely many maps. With the term *bilinear* we express the following properties for any u, v, x and $y \in R^n$ and any a, $b \in R$ we get

$$\begin{aligned} \langle au+v,x\rangle &= a\langle u,x\rangle + \langle v,x\rangle \\ \langle u,bx+y\rangle &= b\langle u,x\rangle + \langle u,y\rangle \end{aligned}$$

The term *symmetric* clearly refers to $\langle x,y\rangle = \langle y,x\rangle$ for any x, $y \in R^n$ and *form* is reserved for maps that go down to the base ring. Also if $x \in R^n$, $y \in R^m$ and $A \in \mathrm{mat}_{m,n}(R)$ then we get

$$\langle Ax,y\rangle \ = \ \langle x,A^*y\rangle$$

where A^* is the transpose of A. All this has been established in section 4.1. If $R = \mathbb{R}$ is the field of reals, the scalar product has another important property - it is *positive*: For any $x_i \in \mathbb{R}$ we find

$$\langle x,x\rangle \ = \ \sum_{i=1}^{n} x_i^2 \ \geq \ 0$$

In fact the scalar product even is *positive definite*, that is for any $x \in \mathbb{R}^n$ we also have the equivalence

$$\langle x,x\rangle \ = \ 0 \ \iff \ x \ = \ 0$$

Prob If $x = 0$ then $\langle x,x\rangle = 0$ is clear. Conversely if we had $x_1 \neq 0$ (for example) then $x_1^2 > 0$. And as $x_i^2 \geq 0$ for any $i \in 2 \ldots n$ there is no negative number in $\langle x,x\rangle = x_1^2 + x_2^2 + \cdots + x_n^2$ to cancel x_1^2 such that $\langle x,x\rangle > 0$ as well. Therefore $\langle x,x\rangle = 0$ implies $x_i = 0$ for all $i \in 1 \ldots n$.

(4.91) Definition:
Now consider $\mathbb{C}^n$ for some $1 \leq n \in \mathbb{N}$ and $w = (w_1, w_2, \ldots, w_n)$ and $z = (z_1, z_2, \ldots, z_n) \in \mathbb{C}^n$. Then we define the **inner product** on $\mathbb{C}^n$ to be the following map

$$\mathbb{C}^n \times \mathbb{C}^n \ :\to \ \mathbb{C} \ : \ (w,z) \ \mapsto \ \langle w \mid z\rangle \ := \ \sum_{k=1}^{n} w_k \overline{z}_k$$

And if $A = (a_{i,j}) \in \mathrm{mat}_{m,n}(\mathbb{C})$ is an $(m \times n)$-matrix over the complex numbers, then we define the **complex conjugate** matrix $\overline{A}$ of A to be the transpose matrix of A in which all entries are conjugated

$$\overline{A} \ := \ \left(\overline{a}_{j,i}\right) \ \in \ \mathrm{mat}_{n,m}(\mathbb{C})$$

(4.92) Proposition: (viz. 936)

Let $1 \leq m, n \in \mathbb{N}$, then the inner product on $\mathbb{C}$ is a *sesqui-linear form* of $\mathbb{C}^n$ with respect to the complex conjugation. That is for any $t, w, z \in \mathbb{C}^n$ and any $a, b \in \mathbb{C}$ we get

$$\begin{aligned}
\langle t + w \mid z \rangle &= \langle t \mid z \rangle + \langle w \mid z \rangle \\
\langle t \mid w + z \rangle &= \langle t \mid z \rangle + \langle t \mid w \rangle \\
\langle aw \mid z \rangle &= a\langle w \mid z \rangle \\
\langle w \mid bz \rangle &= \overline{b}\langle w \mid z \rangle \\
\langle z \mid w \rangle &= \overline{\langle w \mid z \rangle}
\end{aligned}$$

If we extend the maps of the *real* and *imaginary part* and the complex conjugation of $\mathbb{C}$ to $\mathbb{C}^n$ componentwise by letting [as always, we take $z = (z_1, z_2, \ldots, z_n) \in \mathbb{C}^n$ in the equations below]

$$\begin{aligned}
\mathrm{re}(z) &:= \big(\mathrm{re}(z_1), \mathrm{re}(z_2), \ldots, \mathrm{re}(z_n)\big) \in \mathbb{R}^n \\
\mathrm{im}(z) &:= \big(\mathrm{im}(z_1), \mathrm{im}(z_2), \ldots, \mathrm{im}(z_n)\big) \in \mathbb{R}^n \\
\overline{z} &:= \big(\overline{z}_1, \overline{z}_2, \ldots, \overline{z}_n\big) \in \mathbb{C}^n
\end{aligned}$$

then the inner product and scalar product are related $\langle w \mid z \rangle = \langle w, \overline{z} \rangle$ and we also get the following identities for the real and imaginary parts of the inner product

$$\begin{aligned}
\mathrm{re}\big(\langle w \mid z \rangle\big) &= \langle \mathrm{re}(w), \mathrm{re}(z) \rangle + \langle \mathrm{im}(w), \mathrm{im}(z) \rangle \\
\mathrm{im}\big(\langle w \mid z \rangle\big) &= \langle \mathrm{im}(w), \mathrm{re}(z) \rangle - \langle \mathrm{re}(w), \mathrm{im}(z) \rangle
\end{aligned}$$

In particular the inner product is positive definite again, that is for any $z \in \mathbb{C}^n$ we have $\langle z \mid z \rangle \in \mathbb{R}^+$ is a positive real number, and we also get the equivalence of

$$\langle z \mid z \rangle = 0 \iff z = 0$$

Finally, if $w \in \mathbb{C}^n$, $z \in \mathbb{C}^m$ and $A \in \mathrm{mat}_{m,n}(\mathbb{C})$ then we get the following identity of the inner products $\langle A\, w \mid z \rangle$ of $\mathbb{C}^m$ and $\langle w \mid \overline{A}\, z \rangle$ of $\mathbb{C}^n$ respectively

$$\langle A\, w \mid z \rangle = \langle w \mid \overline{A}\, z \rangle$$

Let us generalize these two notions: Both the scalar product and the inner product are maps of the form $s : M \times M \to R$ where M is $\mathbb{R}^n$ or $\mathbb{C}^n$ and R is the base field $\mathbb{R}$ or $\mathbb{C}$ respectively. Both maps are linear in the first argument, but in the second argument there can be some twist of the base field. To be positive definite means that the images $s(x, x)$ are squares in the base field. Therefore we find the following common concept:

(4.93) Definition: (viz. 936)
Let $(R,+,\cdot)$ be a commutative ring, $\varepsilon \in \mathrm{rend}(R)$ be an endomorphism of R and M be an R-module. Then a map of the following form

$$s \;:\; M \times M \to R \;:\; (x,y) \mapsto s(x \mid y)$$

is said to be a **sesqui-linear** form with **respect to** ε [the word *sesqui* is derived from latin, meaning *one-and-a-half*], iff it satisfies the following three properties for any $x, y, z \in M$ and any $a \in R$

(1) $s(ax \mid y) \;=\; a \cdot s(x \mid y)$

(2) $s(x+y \mid z) \;=\; s(x \mid z) + s(y \mid z)$

(3) $s(y \mid x) \;=\; \varepsilon\big(s(x \mid y)\big)$

Note that a sesqui-linear form with respect to $\varepsilon = \mathbb{1}_R$ is the same as a symmetric bilinear form. Generally, for any sesqui-liear form we already get the following additional properties

(4) $s(x \mid ay) \;=\; \varepsilon(a) \cdot s(x \mid y)$

(5) $s(x \mid y+z) \;=\; s(x \mid y) + s(y \mid z)$

The sesqui-linear form s is said to be **positive definite**, iff for any $x \in M$ with $x \neq 0$ there is some unit $a \in R^*$, such that $s(x \mid x)$ is of the form $s(x \mid x) = a \cdot \varepsilon(a)$. Formally that is

$$x \;=\; 0 \quad \text{or} \quad s(x \mid x) \;\in\; \{\, a \cdot \varepsilon(a) \mid a \in R^* \,\}$$

If $P \;\leq_{\mathrm{m}}\; M$ is a sub-module of M and $s : M \times M \to R$ is any sesqui-linear form on M, then we define the **orthogonal complement** of P to be the following sub-module of M

$$P^{\perp} \;:=\; \{\, x \in M \mid \forall\, p \in P \;:\; s(x \mid p) = 0 \,\} \;=\; \bigcap_{p \in P} \mathrm{kn}\,(x \mapsto s(x \mid p))$$

If there are several sesqui-linear forms involved we will also write $s(\perp \mid P)$ instead of $P^{\perp}$ in order to fix the form used in the construction. Now a subset $\{\, m_i \mid i \in I \,\} \subseteq M$ is said to be an **orthonormal basis** (abbreviated as **ONB**) of M with **respect to** s, iff it satisfies

(1) $\{\, m_i \mid i \in I \,\}$ is an R-basis of M and

(2) $\forall\, i, j \in I$ we get $s(m_i \mid m_j) = \delta_{i,j}$

If $\{\, m_i \mid i \in I \,\}$ is an orthonormal basis with respect to some symmetric bilinear form $b : M \times M \to R$, then we will sometimes omit the "with respect to" part, if b is understood.

(4.94) Remark:
Let us take a look at the set $Q := \{\, a \cdot \varepsilon(a) \mid a \in R^* \,\}$: As ε is a homomorphism of rings we find $Q \subseteq R^*$ as the inverse element of $a\varepsilon(a) \in Q$ is just $a^{-1}\varepsilon(a^{-1}) \in Q$. If $\varepsilon = \mathbb{1}$ then Q is just the positive cone $Q = \{\, a^2 \mid a \in R^* \,\}$. In case $R = \mathbb{R}$ this is $Q = \mathbb{R}_{>0}$. And in case $R = \mathbb{C}$ under the complex conjugation $\varepsilon = \kappa$ we also have $Q = \mathbb{R}_{>0}$.
The reason we need this set is the Gram-Schmidt orthonormalization (4.97). Here we will use some $r(x) \in R^*$ such that $s(x,x) = r(x)\,\varepsilon r(x)$. In both cases $R = \mathbb{R}$ and $R = \mathbb{C}$ (and s is the scalar, resp. the

inner product) we may take $r(x) = \sqrt{\langle x \mid x \rangle}$ to do so. Later on we will take this for the definition of the norm of x and interpret this expression as the length of $x \in \mathbb{C}^n$.

(4.95) Example:

(i) The scalar product $\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ is a sesqui-linear form on the $\mathbb{R}$-vector-space $\mathbb{R}^n$ [with respect to the identity map on $\mathbb{R}$]. It is positive definite, as for all $x \in \mathbb{R}^n$ with $x \neq 0$ we have $\langle x, x \rangle > 0$ and thereby we have $r \in \mathbb{R}^*$ and $r^2 = \langle x, x \rangle$ for the square root

$$r \;=\; \sqrt{\langle x, x \rangle} \;\in\; \mathbb{R}_{>0}$$

(ii) In fact for any matrix $A \in \mathrm{mat}_n(\mathbb{R})$ with $A = A^*$ the map $b(x \mid y) := \langle Ax, y \rangle$ is a symmetric bilinear form on $\mathbb{R}$ and hence a sesqui-linear form. However b need not be positive definite unless A satisfies further properties. We will later see, that a matrix A whose eigenvalues are all strictly positive will make a positive definite b.

(iii) The inner product $\mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}$ is a sesqui-linear form on the $\mathbb{C}$-vector-space $\mathbb{C}^n$ [with respect to the complex conjugation κ on $\mathbb{C}$]. It is positive definite for the same reason as in (i). The scalar product on $\mathbb{C}^n$ is not positive definite, as $\langle z, z \rangle = 0$ does not imply $z = 0$.

(iv) As in (ii) the map $s(x \mid y) := \langle Ax \mid y \rangle$ for some matrix $A \in \mathrm{mat}_n(\mathbb{C})$ that satisfies satisfies $A = \overline{A}$ is a sesqui-linear form with respect to the complex conjugation κ. As in (ii) we have to imposes further restrictions on A to guarantee that s is positive definite.

(v) Item (iii) can be generalized: If $b : R^n \times R^n \to R$ is a symmetric bilinear form and $\varepsilon \in \mathrm{rend}(R)$ is some endomorphism of the ring R with $\varepsilon^2 = \mathbb{1}_R$ (in particular ε is bijective), then we let $\varepsilon(x) := (\varepsilon(x_1), \ldots, \varepsilon(x_n))$ for any $x = (x_1, \ldots, x_n) \in R^n$ and $s(x \mid y) := b(x, \varepsilon(y))$. Thereby s is a sesqui-linear form, with respect to ε.

(vi) If V is a finite-dimensional $\mathbb{R}$-vector-space, then V admits a positive definite, symmetric, bilinear form b: Just choose a basis $\{ v_1, \ldots, v_n \}$ of V. Then there is a isomorphism of vector-spaces

$$\Phi \;:\; \mathbb{R}^n \to V \;:\; (x_1, \ldots, x_n) \mapsto \sum_{k=1}^{n} x_k v_k$$

And thereby we can define the bilinear form $b : V \times V \to \mathbb{R}$ (that depends on the choice of the basis) by pulling back the scalar product from $\mathbb{R}^n$, that is for $u, v \in V$ we let

$$b(u \mid v) \;:=\; \langle \Phi^{-1}(u), \Phi^{-1}(u) \rangle$$

(vii) Likewise if V is a finite-dimensional $\mathbb{C}$-vector-space, then V admits a positive definite, sesqui-linear form s with respect to κ: As in (vi) we choose a basis of V and take $\Phi : \mathbb{C}^n \xrightarrow{\sim} V$. Then for $u, v \in V$ we let

$$s(u \mid v) \;:=\; \langle \Phi^{-1}(u) \mid \Phi^{-1}(v) \rangle$$

(viii) Let $M := \mathrm{mat}_{m,n}(R)$ and for $A, B \in M$ define $b(A \mid B) := \mathrm{tr}(AB^*)$, then b is a symmetric bilinear form. Specifically for $R = \mathbb{C}$ we may take $s(A \mid B) := \mathrm{tr}(A\overline{B})$, then s is a sesqui-linear form on M

with respect to κ. In fact $b(A \mid B)$ is given by

$$b(A \mid B) \;:=\; \mathrm{tr}(AB^*) \;=\; \sum_{i=1}^{m} \langle \mathrm{row}_i(A),\, \mathrm{row}_i(B) \rangle$$

(ix) Let $M := C([a,b], \mathbb{R})$ be the $\mathbb{R}$-vector space of continuous functions of the form $f : [a,b] \to \mathbb{R}$. Then we obtain a symmetric bilinear form on M by letting

$$b(f \mid g) \;:=\; \int_a^b f(x) \cdot g(x)\, dx$$

Likewise for the $\mathbb{C}$-vector-space $M = C([a,b], \mathbb{C})$ of continuos functions of the form $f : [a,b] \to \mathbb{C}$, then in complete analogy, we obtain a sesqui-linear form on M, by letting

$$s(f \mid g) \;:=\; \int_a^b f(x) \cdot \overline{g(x)}\, dx$$

(4.96) Example:
For any commutative ring $(R, +, \cdot)$ the Euclidean basis $\{ e_1, \ldots, e_n \}$ is an ONB of R^n with respect to the scalar product on R^n. In $\mathbb{C}^n$ the Euclidean basis $\{ e_1, \ldots, e_n \}$ also is an ONB of $\mathbb{C}^n$ with respect to the inner product on $\mathbb{C}^n$. However an ONB need not be unique: For example in the case $R = \mathbb{R}$ or $R = \mathbb{C}$ and $n = 2$ there is another ONB of R^2, namely

$$\left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix},\; \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}$$

(4.97) Theorem: (viz. 938)
Let $(R, +, \cdot)$ be a commutative ring with a fixed endomorphism $\varepsilon \in \mathrm{rend}(R)$. Also let s be a sesqui-linear form with respect to ε on the R-module M. Then

(i) A subset $\{ m_i \mid i \in I \} \subseteq M$ already is linear independent, if it is an *ortho-normal system* of M with respect to s, that is if it satisfies

$$\forall\, i, j \in I \;:\; s(m_i \mid m_j) \;=\; \delta_{i,j}$$

(ii) If $\{ m_i \mid i \in I \}$ is an ONB with respect to s then for any $x \in M$ the coefficients of the basis representation of x are given by $s(x \mid m_i)$ and therefore

$$x \;=\; \sum_{i \in I} s(x \mid m_i)\, m_i$$

(iii) If M is a free, finitely generated R-module and s is positive definite, then M has an ONB $\{ g_1, \ldots, g_n \}$ with respect to s. And this can be gained in the following way:

Gram-Schmidt-Orthonormalisation: If $\{ m_1, \ldots, m_n \}$ is a basis of M, then the following algorithm generates generates the ONB $\{ g_1, \ldots, g_n \}$ out of $\{ m_1, \ldots, m_n \}$: For any $0 \neq x \in M$ there is some $r(x) \in R^*$ with $r(x) \cdot \varepsilon(r(x)) = s(x \mid x)$. Now define

$$N(x) \;:=\; \begin{cases} r(x)^{-1} x \text{ if } x \neq 0 \\ 0 \text{ if } x = 0 \end{cases} \;\in\; M$$

and start with $g_1 := N(m_1)$. For $k \in 2 \ldots n$ suppose we have already constructed $\{ g_1, \ldots, g_{k-1} \}$ then g_k is taken to be following element of M

$$g_k \;:=\; N\left(m_k - \sum_{i=1}^{k-1} s(m_k \mid g_i)\, g_i \right)$$

Then $\{ g_1, \ldots, g_n \}$ is an ONB of M with respect to s and for any $k \in 1 \ldots n$ this basis also satisfies

$$\mathrm{Lh}\{ g_1, \ldots, g_k \} \;=\; \mathrm{Lh}\{ m_1, \ldots, m_k \}$$

(4.98) Corollary: (viz. 939)
Let $(F, +, \cdot)$ be a field, $\varepsilon \in \mathrm{rend}(F)$ be an endomorphism of F, V be a finite-dimensional F-vector-space and s be a positive definite sesqui-linear form on V (with respect to ε). Recall the definition of the orthogonal complement of some subspace $U \leq_{\mathrm{v}} V$ of V

$$U^\perp \;=\; \{ x \in V \mid \forall\, u \in U \,:\, s(x \mid u) = 0 \} \;=\; \bigcap_{u \in U} \mathrm{kn}\,(x \mapsto s(x \mid u))$$

Then $U^\perp \leq_{\mathrm{v}} V$ is another subspace and V is the inner direct sum of U and $U^\perp$. Finally the orthogonal complement of $U^\perp$ is U again. Together these are the following two properties

$$\begin{aligned} V &= U \oplus U^\perp \\ (U^\perp)^\perp &= U \end{aligned}$$

And thereby V has an ONB $\{ g_1, \ldots, g_r, \ldots, g_n \} \subseteq V$ with respect to s that splits V into the subspaces U and $U^\perp$. That is, there is some $r \in 0 \ldots n$ such that we get

$$\begin{aligned} U &= \mathrm{Lh}\{ g_1, \ldots, g_r \} \\ U^\perp &= \mathrm{Lh}\{ g_{r+1}, \ldots, g_n \} \end{aligned}$$

(4.99) Definition:
Let $(R, +, \cdot)$ be a commutative ring and M, N be R-modules. Then we introduce the following notions:

(i) The set of all linear forms $f : M \to R$ [which is an R-module itself, according to (3.71.(v))] is called the **dual space** of M and we denote it by

$$M' \;:=\; \mathrm{mhom}_R(M, R)$$

(ii) As M' is an R-module again, we may define the **bidual** M'' of M to be the dual space of the dual

space of M: $M'' := (M')' = \mathrm{mhom}_R(M', R)$. Thus we obtain the **natural map**

$$\beta \ : \ M \to M'' \ : \ x \mapsto \big(f \mapsto f(x)\big)$$

that is $\beta(x)(f) = f(x) \in R$. Clearly this is a homomorphism of R-modules again and M is said to be **reflexive**, iff this β even is an isomorphism.

(iii) A map of the form $\delta : M \times N \to R$ is said to be a **duality** of M and N, iff it is linear in the first argument and additive in the second argument. That is for any $u, v \in M$, $x, y \in N$ and $a \in R$

(1) $\delta(au, x) \ = \ a \cdot \delta(u, x)$

(2) $\delta(u + v, x) \ = \ \delta(u, x) + \delta(v, x)$

(3) $\delta(u, x + y) \ = \ \delta(u, x) + \delta(u, y)$

Note that the properties (1) and (2) just state that for any $x \in N$ the map $u \mapsto \delta(u, x)$ is linear and thereby we obtain a natural map

$$N \to M' \ : \ x \mapsto \delta_x \quad \text{where} \quad \delta_x(u) = \delta(u, x)$$

(iv) The ordered pair (M, N) is said to be a **dual pair** of modules **under the duality** δ iff it satisfies the following three properties

(1) $\delta : M \times N \to R$ is a duality

(2) $\forall\, u \in M \ : \ \big(\forall\, x \in N : \delta(u, x) = 0\big) \implies u = 0$

(3) $\forall\, x \in N \ : \ \big(\forall\, u \in M : \delta(u, x) = 0\big) \implies x = 0$

(v) Let M_1, M_2, N_1 and N_2 be R-modules and let $\varphi_1 : M_1 \to N_1$ and $\varphi_2 : N_2 \to M_2$ be R-linear maps. If also (M_1, M_2) is a dual pair under δ_M and (N_1, N_2) is a dual pair under δ_N, then we say that φ_2 is **conjugate** or **adjoint** to φ_1 iff for any $u \in M_1$ and any $y \in N_2$

$$\delta_M\big(u, \varphi_2(y)\big) \ = \ \delta_N\big(\varphi_1(u), y\big)$$

In this case (if it exists) φ_2 is uniquely determined by φ_1 and we therefore write $\varphi_1' := \varphi_2$ for it.

Prob Suppose both $\varphi_2 : N_2 \to M_2$ and $\overline{\varphi}_2 : N_2 \to M_2$ are adjoint maps of φ_1. In particular we have $\delta_M(u, \varphi_2(y)) = \delta_M(u, \overline{\varphi}_2(y))$ for any $u \in M$ and any $y \in N_2$. But as (M_1, M_2) is a dual pair under δ_M we may subtract to find $\delta_M(u, \varphi_2(y) - \overline{\varphi}_2(y)) = 0$, As this is true for any $u \in M_1$ we get $\varphi_2(y) - \overline{\varphi}_2(y) = 0$. This again is $\varphi_2(y) = \overline{\varphi}_2(y)$ for any $y \in N_2$ such that $\varphi_2 = \overline{\varphi}_2$ is unique.

(4.100) Remark:

(i) By definition the second argument $N \to M' : u \mapsto \delta(u,x)$ of a duality $\delta : M \times N \to R$ is a homomorphism from the additive group $(M,+)$ to the additive group $(R,+)$. In particular we have

(4) $\forall\, u \in M \;:\; \delta(u,0) = 0$

(5) $\forall\, u \in M\, \forall\, x \in N \;:\; \delta(u,-x) = -\delta(u,x)$

Prob As $\delta(u,0) = \delta(u,0+0) = \delta(u,0) + \delta(u,0)$ we find $\delta(u,0) = 0$ by subtracting $\delta(u,0)$ once. And thereby $0 = \delta(u,0) = \delta(u,x-x) = \delta(u,x) + \delta(u,-x)$ such that $\delta(u,-x) = -\delta(u,x)$, as well.

(ii) If $b : M \times N \to R$ is a bilinear map, then b already is a duality of M and N. Likewise if $s : M \times M \to R$ is a sesqui-linear form with respect to some endomorphism $\varepsilon \in \mathrm{rend}(R)$, then s is a duality of M with itself. In particular

$$\begin{aligned} R^n \times R^n \to R &\;:\; (x,y) \mapsto \langle x,y\rangle \\ \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C} &\;:\; (w,z) \mapsto \langle w \mid z\rangle \end{aligned}$$

are dualities of R^n resp. of $\mathbb{C}^n$ with itself. Thereby (R^n, R^n) even is a dual pair under the scalar product and $(\mathbb{C}^n, \mathbb{C}^n)$ also is a dual pair under the inner product.

Prob Everything is trivial, but the claim of the dual pairs: For this we pick up the Euclidean basis $\{ e_1, \ldots, e_n \} \subseteq R^n$. Then for any $u = (u_1, \ldots, u_n) \in R^n$ we have $u_k = \langle u, e_k\rangle$. Thus we have property (2) of a dual pair. Likewise property (3) follows from $x_k = \langle e_k, x\rangle$ for any $x = (x_1, \ldots, x_n) \in R^n$. The proof for $\mathbb{C}^n$ is exactly the same.

(iii) For any R-module M we find a bilinear map (in particular a duality) of M and its dual space M' by virtue of

$$M \times M' \to R \;:\; (x,f) \mapsto f(x)$$

Prob As $f \in M'$ is linear we get $(ax+y, f) \mapsto f(ax+y) = af(x) + f(y)$ which is the linearity in the first argument. And as M' is equipped with point-wise operations we also get $(x, af+g) \mapsto (af+g)(x) = af(x) + g(x)$ which is the linearity in the second argument.

(iv) (■) The following example is taken from integration theory, it is not needed four our purposes: Let (X, Σ, μ) be a *measure space*, that is X is a non-empty set, Σ a σ-algebra on X and μ a measure of Σ. For any $1 \leq p \in \mathbb{R}$ there is the $\mathbb{R}$-vector-space of *p-times integrable* functions

$$L^p(X,\mu) \;:=\; \{ f : X \to \mathbb{R} \mid |f|^p \text{ is Lebesgue-integrable} \}$$

Now let $1 \leq p, q \in \mathbb{R}$ with $1/p + 1/q = 1$, then by the Hölder-inequality (e.g. refer to Bauer, Maß- und Integrationstheorie, 14.6) we obtain the dual pair $(L^p(X,\mu), L^q(X,\mu))$ under the duality

$$L^p(X,\mu) \times L^q(X,\mu) \to \mathbb{R} \;:\; (f,g) \mapsto \int_X |f(x) \cdot g(x)|\, d\mu(x)$$

(4.101) Proposition: (viz. 941)
Let $(R, +, \cdot)$ be a commutative ring and M and N be R-modules. Then the following statements are true:

(i) If $\{ m_1, \ldots, m_n \}$ is an R-base of M, then $\{ m'_1, \ldots, m'_n \}$ is an R-base of the dual space M' (called the **dual base** of $\{ m_1, \ldots, m_n \}$), where for any $j \in 1 \ldots n$ the element $m'_j \in M'$ is defined by

$$m'_j \ : \ M \to R \ : \ \sum_{i=1}^{n} a_i \, m_i \mapsto a_j$$

Nota that this statement can not be generalized to infinite dimensions. Even over a field the dual space V' over an infinite-dimensional vector-space V will exceed V in dimension, as the m'_j form a linearly independent set, that does not generate V' however.

(ii) Let $\{ m_1, \ldots, m_n \} \subseteq M$ be a basis of M and $\{ m'_1, \ldots, m'_n \} \subseteq M'$ be its dual basis. Likewise let $\{ m''_1, \ldots, m''_n \} \subseteq M''$ be the dual basis of $\{ m'_1, \ldots, m'_n \}$, then we find that (for any $k \in 1 \ldots n$)

$$\beta(m_k) \ = \ m''_k$$

(iii) If M is a free R-module then the natural map $\beta : M \to M''$ is injective. If M is free and finitely generated, then β even is bijective. In particular any free, finitely generated module is reflexive.

(iv) For any R-module M the following three statements are equivalent

(a) the natural map β is injective

(b) (M, M') is a dual pair under $\delta(x, f) := f(x)$

(c) $\forall\, x \in M \ : \ \big(\forall\, f \in M' : f(x) = 0\big) \implies x = 0$

(v) Let $\delta : M \times N \to R$ be any map and for $x \in N$ denote $\delta_x : M \to R$ defined by $\delta_x(u) := \delta(u, x)$ again. Also let $\mathrm{im}(\delta) := \{ \delta_x \mid x \in N \}$ then (M, N) is a dual pair under δ if and only if

(1) $\delta : M \times N \to R$ is a duality

(2') $\forall\, u \in M \ : \ \big(\forall\, f \in \mathrm{im}(\delta) : f(u) = 0\big) \implies u = 0$

(3') the natural map $N \to M' : x \mapsto \delta_x$ is injective

(vi) Fix an automorphism $\varepsilon \in \mathrm{aut}(R)$ of the ring R and $s : M \times M \to R$ a positive definite sesqui-linear form on M with respect to ε. Assume that M is free and finitely generated then the following map

$$S \ : \ M \to M' \ : \ y \mapsto \big(x \mapsto s(x \mid y)\big)$$

not only is well-defined and ε-linear, but also is bijective. Recall that ε-linear means that for any $y, z \in M$ and any $a \in R$ we get

$$\begin{aligned} S(ay) &= \varepsilon(a) S(y) \\ S(y + z) &= S(y) + S(z) \end{aligned}$$

Remark: Note that S is well-defined and ε-linear for any sesqui-linear form S and any module M. If s is positive definite, then S already is injective. Also note that if R is noetherian and ε is surjective, then ε already is bijective, as well, according to (3.82.(i)).

(4.102) Remark:
With this knowledge in mind let us return to the definition of the adjoint of a homomorphism of R-modules:

(i) Recall the notation of (4.99.(v)) and let us present a diagram of what it means that $\varphi_2 : N_2 \to M_2$ is the adjoint of some module homomorphism $\varphi_1 : M_1 \to N_2$

$$\begin{array}{ccccccc} \delta_M & : & M_1 & \times & M_2 & \to & R \\ & & \downarrow \varphi_1 & & \uparrow \varphi_2 & & \\ \delta_N & : & N_1 & \times & N_2 & \to & R \end{array}$$

(ii) This definition is usually applied to the following case: If M is a free R-module then the natural map $\beta : M \to M''$ is injective and hence (M, M') is a dual pair under $\delta(x, f) := f(x)$ - according to (4.101) again. Let us fix this duality, then we get

$$\begin{array}{ccccccccc} M & \times & M' & \to & R & : & (x,f) & \mapsto & f(x) \\ \downarrow \varphi & & \uparrow \varphi' & & & & & & \\ N & \times & N' & \to & R & : & (y,g) & \mapsto & g(y) \end{array}$$

If M and N are free R-modules and $\varphi : M \to N$ is a linear map, then $\varphi' : N' \to M'$ is the adjoint map of φ if and only if

$$\forall\, g \in N' \;:\; g\varphi \;=\; \varphi'(g) \;\in\; M'$$

Prob for any $u \in M$ and $g \in N'$ we have $\beta(\varphi(u), g) = g(\varphi(u)) = g\varphi(u)$ and likewise $\beta(u, \varphi'(g)) = \varphi'(g)(u)$. If φ' is the adjoint of φ then these are equal $g\varphi(u) = \varphi'(g)(u)$ and as $u \in M$ has been arbitrary this is the equality of maps $g\varphi \;=\; \varphi'(g)$.

(iii) If $(R, +, \cdot)$ is a commutative ring and $1 \leq m, n \in \mathbb{N}$ then (R^m, R^m) and (R^n, R^n) are a dual pairs under the respective scalar products. Let now $\varphi : R^n \to R^m$ be given by the matrix $A \in \mathrm{mat}_{m,n}(R)$, that is $\varphi(x) = Ax$ for any $x \in R^n$. Then the adjoint φ' of φ is given to be the transpose matrix A^* of A, as $\langle x, \varphi'(y)\rangle = \langle x, A^*y\rangle = \langle Ax, y\rangle = \langle \varphi(x), y\rangle$ is true for any $x \in R^n$ and $y \in R^m$

$$\varphi' \;:\; R^m \to R^n \;:\; y \mapsto A^*y$$

(iv) Specifically for $R = \mathbb{C}$ we also have the dual pairs $(\mathbb{C}^m, \mathbb{C}^m)$ and $(\mathbb{C}^n, \mathbb{C}^n)$ respective inner products. Again, if $\varphi : \mathbb{C}^n \to \mathbb{C}^m$ is given by the matrix $A \in \mathrm{mat}_{m,n}(R)$, that is $\varphi(x) = Ax$ for any $x \in \mathbb{C}^n$, then the adjoint map φ' of φ is given to be the complex conjugate matrix $\overline{A}$ of A, as $\langle x \mid \varphi'(y)\rangle = \langle x \mid \overline{A}\, y\rangle = \langle Ax \mid y\rangle = \langle \varphi(x) \mid y\rangle$ is true for any $x \in \mathbb{C}^n$ and $y \in \mathbb{C}^m$

$$\varphi' \;:\; \mathbb{C}^m \to \mathbb{C}^n \;:\; y \mapsto \overline{A}\, y$$

(v) Let M is an R-module and consider $b : M \times M \to R$ a bilinear map on M (e.g. the scalar product in case of $M = R^n$). As always there also is the natural map $\beta : M \times M' : (x, f) \mapsto f(x)$. Now, if $P \leq_{\mathsf{m}} M$ is any sub-module of M we would like to compare the orthogonal complements of P with respect to b and to β, these are

$$\begin{aligned} b(P\,|\bot) &= \{\, y \in M \mid \forall\, x \in P : b(x \mid y) = 0 \,\} \\ \beta(P\,|\bot) &= \{\, f \in M' \mid \forall\, x \in P : f(x) = 0 \,\} \end{aligned}$$

Note that $b(P\,|\bot) \leq_{\mathsf{m}} M$ and $\beta(P\,|\bot) \leq_{\mathsf{m}} M'$ so they seem to be completely separate concepts, so far. But according to (4.101.(vi)) b induces a canonical homomorphism of the form

$$b' \,:\, M \xrightarrow{\sim} M' \,:\, y \mapsto \big(x \mapsto b(x \mid y)\big)$$

and for this it is clear, that $b'\big(b(P\,|\bot)\big) \subseteq \beta(P\,|\bot)$. If M is a finitely generated, free R-module then b' even is an isomorphism, and in this case we even get the equality

$$b'\Big(b(P\,|\bot)\Big) = \beta(P\,|\bot)$$

Without b we could still have chosen a basis $\{m_1, \ldots, m_n\}$ of M and this would have induces an isomorphism $M \xrightarrow{\sim} M'$ by linear expansion of $m_k \mapsto m'_k$. However this isomorphism depends on the choice of the basis, which we express by saying that it is *non-canonical*. Given b the isomorphy is induced by b and this is why we call it *canonical*.

(4.103) Corollary: (viz. 944)

(i) Let $(R, +, \cdot)$ be a commutative ring and $1 \leq m,\, n \in \mathbb{N}$. First of all we fix the scalar product $b_n : R^n \times R^n \to R : (x, y) \mapsto \langle x, y \rangle$ as a bilinear form on R^n and respectively b_m on R^m. If now $A \in \mathrm{mat}_{m,n}(R)$ is any $(m \times n)$-matrix over R and $A^* \in \mathrm{mat}_{n,m}(R)$ is its transpose then

$$\begin{aligned} \mathrm{kn}(A) &= \big(\mathrm{im}\,(A^*)\,\big)^{\bot} \\ \mathrm{kn}(A^*) &= \big(\mathrm{im}\,(A)\,\big)^{\bot} \end{aligned}$$

Let $(R, +, \cdot)$ be a commutative ring, $\varepsilon \in \mathrm{aut}(R)$ be an automorphism of R and M and N be a finitely generated, free R-modules. Say $s : M \times M \to R$ and $t : N \times N \to R$ are positive definite sesqui-linear forms (both with respect to ε) and consider $\varphi : M \to N$ a homomorphism of R-modules. Then we get

(ii) Since s is positive definite we have $M^{\bot} = 0$. Likewise, as t is positive definite we have $N^{\bot} = 0$

$$\begin{aligned} M^{\bot} &= \{\, u \in M \mid \forall\, v \in M : s(u \mid v) = 0 \,\} &&= \{0\} \\ N^{\bot} &= \{\, x \in N \mid \forall\, y \in N : t(x \mid y) = 0 \,\} &&= \{0\} \end{aligned}$$

(iii) φ has a (uniquely determined) adjoint homomorphism $\varphi' : N \to M$ of R-modules. And if $\mathcal{M}$ and $\mathcal{N}$ are ordered ONB of M and N respectively and $A = [\varphi]^{\mathcal{N}}_{\mathcal{M}}$ is the matrix representation of φ, then φ' has the matrix representation $[\varphi']^{\mathcal{M}}_{\mathcal{N}} = \varepsilon^{-1}(A^*)$ and satisfies (for any $u,\, v \in M$ and $x,\, y \in N$)

$$t\big(\varphi(u) \mid y\big) = s\big(u \mid \varphi'(y)\big)$$

$$t\big(x \mid \varphi(v)\big) \;=\; s\big(\varphi'(x) \mid v\big)$$

(iv) If φ' is the adjoint homomorphism of φ then we have the following identities for the kernels of φ and φ' respectively

$$\begin{aligned} \mathrm{kn}(\varphi) &= \big(\mathrm{im}\,(\varphi')\,\big)^{\perp} \\ \mathrm{kn}(\varphi') &= \big(\mathrm{im}\,(\varphi)\,\big)^{\perp} \end{aligned}$$

(4.104) Proposition: (viz. 943)
Let $(R,+,\cdot)$ be a commutative ring and $\varepsilon \in \mathrm{aut}(R)$ be an automorphism of R. Also let M a finitely generated, free R-module and $\varphi \in \mathrm{end}(m)$ an endomorphism of M. Finally let $s : M \to M \to R$ be a positive definite sesqui-linear form. If $\mathcal{M}$ is an ordered ONB of M let us denote the matrix representations of φ and φ' by $A := [\varphi]_{\mathcal{M}}$ and $A' := [\varphi']_{\mathcal{M}}$ respectively. Then we define:

(i) If A is the matrix representation of φ in the ordered ONB $\mathcal{M}$ of M, then the matrix representation A' of the adjoint endomorphism φ' in the same basis $\mathcal{M}$ is given to be

$$A' \;=\; \varepsilon^{-1}\big(A^*\big)$$

(ii) φ is said to be **self-adjoint**, iff it satisfies one of the following three equivalent properties

(a) $\varphi' = \varphi$

(b) For any ordered ONB $\mathcal{M}$ of M we get $A^* = \varepsilon(A)$

(c) There is an ordered ONB $\mathcal{M}$ of M such that $A^* = \varepsilon(A)$

(iii) φ is said to be **normal**, iff it satisfies one of the following three equivalent properties

(a) $\varphi'\,\varphi \;=\; \varphi\,\varphi'$

(b) For any ordered ONB $\mathcal{M}$ of M we get $\varepsilon^{-1}(A^*)\,A \;=\; A\,\varepsilon^{-1}(A^*)$

(c) There is an ordered ONB $\mathcal{M}$ of M such that $\varepsilon^{-1}(A^*)\,A \;=\; A\,\varepsilon^{-1}(A^*)$

(4.105) Remark:
If φ in (4.104) is sefl-adjoint, but $\mathcal{M}$ is an ordered basis of M, but *not* an ONB, then A need *not* be ε-symmetric [that is satisfy $A^* = \varepsilon(A)$]. As a counter-example regard $\varepsilon = \mathbb{1}$, $M = \mathbb{R}^2$ and the following endomorphism on M:

$$\varphi \;:\; \mathbb{R}^n \to \mathbb{R}^n \;:\; (x,y) \mapsto \big(x+2y,\, 2x+3y\big)$$

It is clear that φ has the following symmetric matrix representation in the euclidean basis $\mathcal{E} = (e_1, e_2)$ of $\mathbb{R}^2$ and hence is self-adjoint, by property (c) in the definition above

$$[\varphi]_{\varepsilon} \;=\; \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}$$

Take a look at another ordered basis $\mathcal{M} := (m_1, m_2)$ where $m_1 := e_1 = (1,0)$ and $m_2 := (1,1)$. In this ordered basis φ does *not* have a symmetric matrix representation, instead

$$[\varphi]_{\mathcal{M}} \;=\; [\mathbb{1}]^{\mathcal{M}}_{\mathcal{E}}[\varphi]_{\mathcal{E}}[\mathbb{1}]^{\mathcal{E}}_{\mathcal{M}} \;=\; \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \;=\; \begin{pmatrix} -1 & -2 \\ 2 & 5 \end{pmatrix}$$

(4.106) Definition:
Let us append a generalization of the concept of an orthogonal complement introduced in (4.98) in the general setting of modules: Let $(R,+,\cdot)$ and $(S,+,\cdot)$ be any rings, α and $\beta : R \to S$ be fixed homomorphisms of rings and consider the R-modules L, M and the S-module N. Finally let b be a map of the form

$$b \;:\; L \times M \;\to\; N$$

that is α-linear in the first and β-linear in the second argument. That is for any $u, v \in L$, any $x, y \in M$ and any $a \in R$ we assume the following identities

$$\begin{aligned} b(u+v \mid x) &= b(u \mid x) + b(v \mid x) \\ b(u \mid x+y) &= b(u \mid x) + b(u \mid y) \\ b(au \mid x) &= \alpha(a)\, b(u \mid x) \\ b(u \mid ax) &= \beta(a)\, b(u \mid x) \end{aligned}$$

That is: If $S = R$ and $\alpha = \beta = \mathbb{1}$, then b is bilinear. For any subsets $P \subseteq L$ and $Q \subseteq M$ we define the **orthogonal complement** of P resp. of Q with respect to b, to be the following sub-modules of M resp. of L

$$Q^{\perp} \;:=\; \{\, u \in L \mid \forall\, q \in Q \,:\, b(u \mid q) = 0 \,\} \;=\; \bigcap_{q \in Q} \mathrm{kn}\big(u \mapsto b(u \mid q)\big)$$

$$P^{\top} \;:=\; \{\, x \in M \mid \forall\, p \in P \,:\, b(p \mid x) = 0 \,\} \;=\; \bigcap_{p \in P} \mathrm{kn}\big(x \mapsto b(p \mid x)\big)$$

In case of ambiguity we also write $b(P \mid \perp) := P^{\top}$ and $b(\perp \mid Q) := Q^{\perp}$ to emphasize the α-β-linear map used in the construction of these sets. Now b is said to be **non-degenerate** iff both $L^{\perp} = 0$ and $M^{\perp} = 0$. That is iff $b(u \mid x) = 0$ for any $x \in M$ is true only for $u = 0$ and likewise $b(u \mid x) = 0$ for any $u \in L$ is true only for $x = 0$. Formally, iff for any $u \in L$ and $x \in M$ we have

$$\begin{aligned} \Big(\forall\, x \in M : b(u \mid x) = 0\Big) \quad &\Longrightarrow \quad u \;=\; 0 \\ \Big(\forall\, u \in L : b(u \mid x) = 0\Big) \quad &\Longrightarrow \quad x \;=\; 0 \end{aligned}$$

A stronger version of this notion is the following: b is said to be **integral**, iff $b(x \mid y) = 0$ implies that $x = 0$ or $y = 0$. That is, iff for any $u \in L$ and $x \in M$ we have the implication

$$b(u \mid x) \;=\; 0 \quad\Longrightarrow\quad u \;=\; 0 \;\text{ or }\; x \;=\; 0$$

(4.107) Proposition: (viz. 940)
As in definition (4.106) above, let $b : L \times M \to N$ be a α-β-linear map from the R-modules L and M to the S-module N. Then we get:

(i) The maps $P \mapsto P^\top$ and $Q \mapsto Q^\perp$ are a Galois connection [refer to (0.22)] between the sets of sub-modules $\mathrm{Subm}(L)$ and $\mathrm{Subm}(M)$ partially ordered under the inclusion $\subseteq$ of sets:

$$\begin{array}{rcl} \mathrm{Subm}(M) & \to & \mathrm{Subm}(M') \\ P & \mapsto & P^\top \\ F^\perp & \hookleftarrow & F \end{array}$$

(ii) We obtain another well-defined map $\overline{b}$, that is non-degenerate, α-linear in the first and β-linear in the second argument, by virtue of

$$\overline{b} \;:\; {}^{L}\big/_{M^\perp} \times {}^{M}\big/_{L^\top} \;\to\; N \;:\; \left(x + M^\perp, y + L^\top\right) \;\mapsto\; b(x,y)$$

(iii) If $(P_i) \subseteq \mathrm{Subm}(L)$ (where $i \in I \neq \emptyset$) and $(Q_j) \subseteq \mathrm{Subm}(M)$ (where $j \in J \neq \emptyset$) and are arbitrary families of sub-modules of L and M respectively, then we get

$$\begin{aligned} \left(\sum_{i\in I} P_i\right)^\top &= \bigcap_{i\in I} P_i^\top \\ \left(\sum_{j\in J} Q_j\right)^\perp &= \bigcap_{j\in J} Q_j^\perp \end{aligned}$$

(iv) Suppose that $\alpha = \beta$ and that b is *integral*, then all elements $x \in L$ and $y \in M$ share the same annihilator and if $x \neq 0$ this is a prime ideal in R. That is we get

$$x \neq 0 \;\text{ and }\; y \neq 0 \quad\Longrightarrow\quad \mathrm{ann}(x) \;=\; \mathrm{ann}(y) \;\in\; \mathrm{Spec}(R)$$

(4.108) Remark:
The standard case of the α-β-linear map b in definition (4.106) is the canonical bilinear map of an R-module M and its dual space M' given by

$$\delta \;:\; M \times M' \to R \;:\; (x,f) \mapsto f(x)$$

Let us repeat the definition of the orthogonal complements of sub-modules $P \leq_{\mathsf{m}} M$ and $F \leq_{\mathsf{m}} M'$ in this case respectively

$$\begin{aligned} P^\top \;=\; \delta(P \mid \perp) \;&:=\; \left\{ f \in M' \mid \forall\, x \in P \,:\, f(x) = 0 \right\} \\ F^\perp \;=\; \delta(\perp \mid F) \;&:=\; \left\{ x \in M \mid \forall\, f \in F \,:\, f(x) = 0 \right\} \end{aligned}$$

This is what inspired our notation: If we consider M' to be one level above M, then $\top$ raises P one level to $P^\top \subseteq M'$. Likewise $\bot$ lowers F one level $F^\bot \subseteq M$. This of course can be iterated, such that $P^{\top\top} \subseteq M''$ for example. However $\beta : M \to M''$ allows to pull back $P^{\top\top}$ onto the level of M.

In this general setting let us consider the following example: The $\mathbb{Z}$-module $M = \mathbb{Z}^3$ is free and finitely generated with basis $\{ e_1, e_2, e_3 \}$. The dual module M' then features the dual basis $\{ e'_1, e'_2, e'_3 \}$. We take a look at its sub-module $P = 3\mathbb{Z} \oplus \mathbb{Z} \oplus 0 = \mathsf{Lh}\{ 3e_1, e_2 \} \leq_\mathsf{m} M$. Thus if we consider any $x = (3a, b, 0) \in P$ and any $f = ue'_1 + ve'_2 + we'_3 \in M'$ then $f(x) = 3au + bv$. In order to have $f \in P^\bot$ we need $f(x) = 0$ for *any* $a, b \in \mathbb{Z}$ and in particular $3u = 0$ and $v = 0$. As $\mathbb{Z}$ is an integral domain this implies $u = 0$ such that $f \in \mathbb{Z}e'_3$. Hence we see

$$\big(\mathbb{Z}\,3e_1 + \mathbb{Z}\,e_2\big)^\top \;=\; \mathbb{Z}\,e'_3$$

Likewise it is clear, that $(\mathbb{Z}e'_3)^\bot = \mathbb{Z}e_1 + \mathbb{Z}e_2$ which is a sub-module of M strictly containing P. Thus - even over a PID - not every sub-module of M satisfies $(P^\top)^\bot = P$ and hence there are sub-modules (like our P here) that are *no* orthogonal complement of some $F \leq_\mathsf{m} M'$.

$$\mathbb{Z}\,3e_1 + \mathbb{Z}\,e_2 \;\subset\; \big(\mathbb{Z}\,3e_1 + \mathbb{Z}\,e_2\big)^{\top\bot}$$

The reason behind this is that $3\mathbb{Z}$ is not complemented in $\mathbb{Z}$ and hence P is not complemented in M. In turn the Galois connection will only be bijective on the set of complemented sub-modules of M, not for all sub-modules.

(4.109) Theorem: (viz. 947)
Let $(R, +, \cdot)$ be a commutative ring and M a finitely generated, free R-module where we fix the bilinear map $M \times M' \to R : (x, f) \mapsto f(x)$. Finally let $P \leq_\mathsf{m} M$ be any sub-module of M, then we get the following statements:

(i) If R is an integral domain and $\{ m_1, \ldots, m_n \}$ is a basis of M such that $\{ a_1 m_1, \ldots, a_r m_r \}$ is a basis of P where $r \in \mathbb{N}$ and $a_1, \ldots, a_r \in R$ then we get the following identities

$$\begin{aligned} P^\top &= \mathsf{Lh}\{ m'_{r+1}, \ldots, m'_n \} \\ P^{\top\bot} &= \mathsf{Lh}\{ m_1, \ldots, m_r \} \;=\; \mathsf{Hull}(P) \end{aligned}$$

Nota that in case of a PID R we know by (5.28.(iv)) there always is a basis $\{ m_1, \ldots, m_n \}$ of M and factors $a_1, \ldots, a_r \in R$ such that $\{ a_1 m_1, \ldots, a_r m_r \}$ is a basis of P.

(ii) Let R be a field and M be a finite-dimensional R-vector space. Then there is a basis $\{ m_1, \ldots, m_n \}$ is a basis of M such that $\{ m_1, \ldots, m_r \}$ is a basis of P (for some $r \in 0 \ldots n$) and thereby

$$\begin{aligned} P^\top &= \mathsf{Lh}\{ m'_{r+1}, \ldots, m'_n \} \\ P^{\top\bot} &= \mathsf{Lh}\{ m_1, \ldots, m_r \} \;=\; P \end{aligned}$$

(iii) Let $\beta : M \to M'' : x \mapsto x''$ be the natural map again, that is x'' is the map $x'' : M' \to R : f \mapsto f(x)$ and consider some sub-modules $P \leq_{\mathsf{m}} M$ and $F \leq_{\mathsf{m}} M'$, then we get the identities

$$\begin{aligned} \beta(P)^{\perp} &= P^{\top} \leq_{\mathsf{m}} M' \\ \beta\left(F^{\perp}\right) &= F^{\top} \leq_{\mathsf{m}} M'' \end{aligned}$$

(iv) If R even is a PID, then the following statements on P are equivalent:

(a) M admits a basis $\{ m_1, \ldots, m_n \}$ such that there is some $r \in \mathbb{N}$ such that the subset $\{ m_1, \ldots, m_r \}$ is a basis of P.

(b) P is *complemented*, that is there is another sub-module $Q \leq_{\mathsf{m}} M$ such that M is the inner direct sum of P and Q

$$M = P \oplus Q$$

(c) There is some sub-module $F \leq_{\mathsf{m}} M'$ of the dual space of M, such that P is the orthogonal complement of F, that is

$$P = F^{\perp}$$

(d) $P = \mathrm{Hull}(P)$

(e) $P = P^{\top\perp}$

(v) If R is a PID again then the Galois connection of (4.107) interlocks the complemented sub-modules of M and M'. That is, if we denote the set of complemented sub-modules of M by

$$\mathrm{Subc}(M) := \{ P \leq_{\mathsf{m}} M \mid \exists Q \leq_{\mathsf{m}} M : M = P \oplus Q \}$$

then going to orthogonal complements yields a bijection between the sets of complemented sub-modules of M and M' respectively. Formally

$$\begin{array}{rcl} \mathrm{Subc}(M) & \longleftrightarrow & \mathrm{Subc}(M') \\ P & \mapsto & P^{\top} \\ F^{\perp} & \hookleftarrow & F \end{array}$$

(4.110) Proposition: (viz. 946)
Let $(R, +, \cdot)$ be a commutative ring M and N be R-modules and consider the following canonical maps concerning the direct sum $M \oplus N$

$$\begin{aligned} \iota_M &: M \hookrightarrow M \oplus N : & x &\mapsto (x, 0) \\ \iota_N &: M \hookrightarrow M \oplus N : & x &\mapsto (x, 0) \\ \pi_M &: M \oplus N \twoheadrightarrow M : & (x, y) &\mapsto x \\ \pi_N &: M \oplus N \twoheadrightarrow N : & (x, y) &\mapsto y \end{aligned}$$

Then we obtain the following isomorphy of the dual space of $M \oplus N$ [note that $f\pi_M + g\pi_N$ is defined by $(f\pi_M + g\pi_N)(x,y) = f(x) + g(y)$]

$$\begin{array}{rcl} (M \oplus N)' & \xrightarrow{\sim} & M' \oplus N' \\ h & \mapsto & (h\iota_M, h\iota_N) \\ f\pi_M + g\pi_N & \leftarrow\!\shortmid & (f,g) \end{array}$$

Likewise we obtain the following isomorphy of the bidual space of $M \oplus N$

$$\begin{array}{rcl} (M \oplus N)'' & \xrightarrow{\sim} & M'' \oplus N'' \\ \omega & \mapsto & \big(f \mapsto \omega(f\pi_M),\, g \mapsto \omega(g\pi_N)\big) \\ \big(h \mapsto \omega_M(h\iota_M) + \omega_N(h\iota_N)\big) & \leftarrow\!\shortmid & (\omega_M, \omega_N) \end{array}$$

And if we denote the natural maps $\beta_M : M \to M'' : x \mapsto (f \mapsto f(x))$ and $\beta_N : N \to N'' : y \mapsto (g \mapsto g(y))$ respectively and likewise $\beta : M \oplus N \to (M \oplus N)'' : (x,y) \mapsto (h \mapsto h(x,y))$ then we get the following commutative diagram $\Theta\beta = \beta_M \times \beta_N$ where

$$\begin{array}{ccc} M \oplus N & & \\ \downarrow & \searrow & \\ (M \oplus N)'' & \xrightarrow{\sim} & M'' \oplus N'' \end{array}$$

$$\begin{array}{rcl} \beta & : M \oplus N \to (M \oplus N)'' : & (x,y) \mapsto (h \mapsto h(x,y)) \\ \beta_M \times \beta_N & : M \oplus N \to M'' \oplus N'' : & (x,y) \mapsto \big(f \mapsto f(x), g \mapsto g(x)\big) \\ \Theta & : (M \oplus N)'' \xrightarrow{\sim} M'' \oplus N'' : & \big(f \mapsto \omega(f\pi_M),\, g \mapsto \omega(g\pi_N)\big) \end{array}$$

(4.111) Corollary: (viz. 949)

(i) Let $(R,+,\cdot)$ be a commutative ring, M and N be R-modules and denote the natural maps β_M, β_N and β as in (4.110). Also let $\star$ abbreviate any of the words *injective*, *surjective* or *bijective*. Then we find the following equivalence:

$$\beta \text{ is } \star \iff \beta_M \text{ and } \beta_N \text{ are } \star$$

(ii) Let $(R,+,\cdot)$ be a commutative ring and M and N be R-modules then $M \oplus N$ is reflexive if and only if both M and N are reflexive.

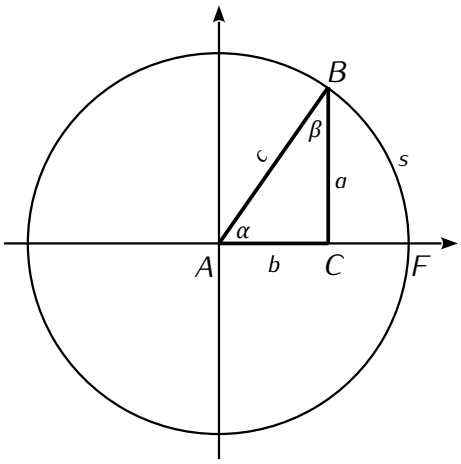
(iii) $(\diamondsuit)$ Let again $(R,+,\cdot)$ be a commutative ring, P be any R-module and $\beta : P \to P''$ be the natural map. Then we find two implications

$$\begin{array}{rcl} P \text{ is projective} & \Longrightarrow & \beta \text{ is injective} \\ P \text{ is projective and finitely generated} & \Longrightarrow & P \text{ is reflexive} \end{array}$$

4.8 Vector Geometry

This section will be quite different from the rest of this textbook, in two ways: First of all we will regard the case of the real numbers as the base field for most of the time, second we will apply our theory to elementary geometry where we will appeal to the mathematical intuition and third we use a few ingredients from basic analysis without proving them. We dare to do so, as from a formal point of view none of this is needed in the rest of the textbook.

The most fundamental concept of geometry is that of a triangle. We find a right-angled triangle inside a circle by connecting the points $A = (0,0)$, $B = (b,a)$ and $C = (b,0) \in \mathbb{R}^2$. The right angle is at point C of course.



It probably is the most commonly known fact of mathematics, that the length of the *hypotenuse* (that is the line from A to B) is closely linked to the length of the legs (that are the lines from C to A and C to B respectively). If you never saw the proof of this, look it up - it is really cute:

(4.112) Lemma: (viz. 1013) **Pythagorean Theorem**
In a rectangular triangle of the points A, B and C, that has its right angle in C and the length of its sides are: a opposite to A, b opposite to B and c opposite to C, we have the relation

$$c^2 = a^2 + b^2$$

The perimeter of the circle (of radius c is) $2\pi c$ (■) . Thus it stands to reason to define the **angle** α at the point A to be the fraction of the length s of the arc from F to B times the radius c of the circle:

$$\alpha := \frac{s}{c} \in [0, 2\pi]$$

This number is independent of the radius and neatly describes the width of the opening of the triangle at A. It is a measure just how far we have to rotate $F = (c,0)$ to reach B. Using this angle we define following functions

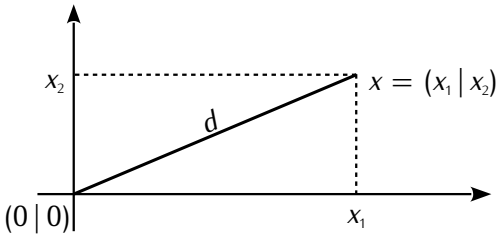
(4.113) Definition:
The **sinus** of the angle α is defined as the ratio of the length of the side opposite to α times the length of the *hypotenuse* of the triangle. The **cosine** of the angle α is defined as the ratio of the length of the side adjacent to α times the length of the hypotenuse:

$$\begin{aligned} \sin(\alpha) &:= \frac{a}{c} \\ \cos(\alpha) &:= \frac{b}{c} \end{aligned}$$

Altogether sinus turns the fraction s/c into the fraction a/c, likewise cosinus that maps $s/c \mapsto b/c$. From the theorem of Pythagoras we then find $\sin(\alpha)^2 + \cos(\alpha)^2 = a^2/c^2 + b^2/c^2 = (a^2+b^2)/c^2 = 1$, which is one of the fundamental properties of these functions:

$$\sin(\alpha)^2 + \cos(\alpha)^2 = 1$$

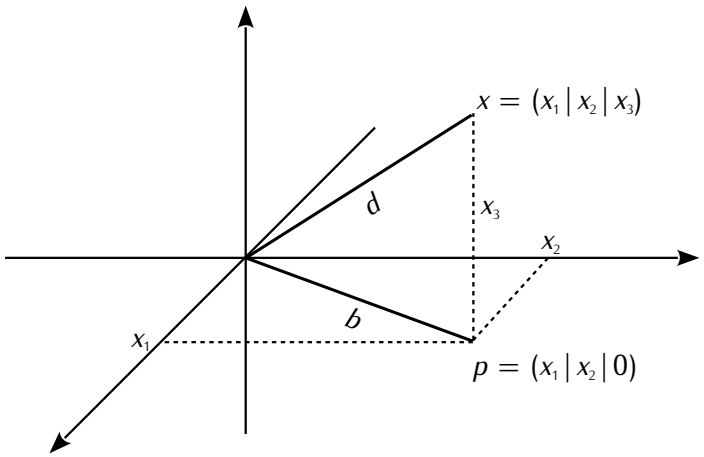
The theorem of Pythagoras also provides a way of measuring distances in a plane: Given a point $x = (x_1, x_2) \in \mathbb{R}^2$ we find, that this point gives rise to a right-angled triangle by looking at its coordinates:



The distance d from $(0 \mid 0)$ to x [in other words the length of the line from $(0 \mid 0)$ to x] can be computed using the Pythagorean theorem

$$d = \sqrt{x_1^2 + x_2^2}$$

We will now generalize this to higher dimensions: Let us take a look at a point $x = (x_1, x_2, x_3) \in \mathbb{R}^3$ in space. We can still illustrate this:



In order to compute the distance d of x from the origin 0 we use the projection $p = (x_1, x_2, 0)$ of x to the level plane. It has distance b from the origin 0. But then another right-angled triangle emerges, having the side lengths b, x_3 and d, where d is the distance of x from 0. Thus we can compute d

$$\begin{aligned} b^2 &= x_1^2 + x_2^2 \\ d^2 &= b^2 + x_3^2 \;=\; x_1^2 + x_2^2 + x_3^2 \end{aligned}$$

So generally in n dimensions we expect $d^2 = x_1^2 + \cdots + x_n^2$. This even is true for $n = 1$, where $\sqrt{x_1^2} = |x_1|$ is just the absolute value of x_1 that measures the distance of x_1 to 0. Therefore we define:

(4.114) Definition:
If $1 \leq n \in \mathbb{N}$ and $x = (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$ is a vector (that is a point in n-dimensional space), then we define the **norm** of x by

$$\|x\| \;:=\; \sqrt{x_1^2 + x_2^2 + \cdots + x_n^2}$$

Likewise for $z = (z_1, z_2, \ldots, z_n) \in \mathbb{C}^n$ we define the **norm** of z to be the norm of the absolute values $(|z_1|, |z_2|, \ldots, |z_n|) \in \mathbb{R}^n$

$$\|z\| \;:=\; \sqrt{|z_1|^2 + |z_2|^2 + \cdots + |z_n|^2}$$

And if $S \subseteq \mathbb{F}^n$ is a subset of n-dimensional space, where $\mathbb{F} \in \{\, \mathbb{R}, \mathbb{C} \,\}$ and $x \in \mathbb{F}^n$ is a point, then $p \in S$ is said to be an **orthogonal projection** of x on S, iff it is a point of least distance in S from x, that is iff

$$\forall\, s \in S \quad \text{we get} \quad \|x - p\| \leq \|x - s\|$$

(4.115) Example:
In the light of the Pythagorean theorem we have to interpret the set of solutions $x = (x_1, x_2) \in \mathbb{R}^2$ of the following equation as a circle or radius $r \geq 0$ around the center $c = (c_1, c_2) \in \mathbb{R}^2$ in the plane $\mathbb{R}^2$

$$(x_1 - c_1)^2 + (x_2 - c_2)^2 \;=\; r^2$$

Likewise in three dimensions: We have to interpret the set of solutions $x = (x_1, x_2, x_3) \in \mathbb{R}^3$ of the following equation as a sphere or radius $r \geq 0$ around the center $c = (c_1, c_2, c_3) \in \mathbb{R}^3$ in the space $\mathbb{R}^3$

$$(x_1 - c_1)^2 + (x_2 - c_2)^2 + (x_3 - c_3)^2 \;=\; r^2$$

It is an interesting observation that geometric objects appear as sets of solutions of certain equations. This is the staging area of differential geometry (if we allow differentiable functions in the equation) and algebraic geometry (if we allow polynomial equations in the equation).
The points that are closer to c, than the radius r form a circle or ball of radius r respectively. That is we have to interpret the set of solutions x of the following inequalities as circle or ball of radius r around the center c respectively:

$$\begin{aligned} (x_1 - c_1)^2 + (x_2 - c_2)^2 &\leq r^2 \\ (x_1 - c_1)^2 + (x_2 - c_2)^2 + (x_3 - c_3)^2 &\leq r^2 \end{aligned}$$

The field of convex geometry is dedicated to studying sets of solutions of linear inequalities. Linear Optimization is the theory of finding the minimum of a linear function over such a set. Generalizing these interpretations we define the $(n-1)$-dimensional **sphere** and n-dimensional **(closed) ball** of radius $r \geq 0$ arund the center $c \in \mathbb{R}^n$ to be the respective set

$$\begin{aligned} S_r(c) &:= \{ x \in \mathbb{R}^n \mid \|x - c\| = r \} \\ B_r(c) &:= \{ x \in \mathbb{R}^n \mid \|x - c\| \leq r \} \end{aligned}$$

(4.116) Definition:
Let $(R, +, \cdot)$ be a commutative ring and M be an R-module. A non-empty subset $S \subseteq M$ is called an **affine space** in M iff it satisfies one of the two following equivalent properties

(a) $\exists\, p \in S$ such that $S - p \leq_{\mathsf{m}} M$ is a sub-module of M

(b) $\forall\, s \in S$ the subset $S - s \leq_{\mathsf{m}} M$ is a sub-module of M

And in this case the sub-modules $S - p = S - s$ are equal for any two $p, s \in S$. Thus if the sub-module $S - s$ is free [e.g. if R is a PID and M is a free, finitely generated R-module] we may define the **dimension** of S to be the dimension of the shifted sub-module $S - s$, formally

$$\dim(S) := \dim(S - s) \text{ for an arbitrary } s \in S$$

Prob We will first show that (a) implies $S - s = S - t$ for any $s, t \in S$. By assumption $P := S - p \leq_{\mathsf{m}} M$ is a sub-module. And if $s \in S$ then clearly $d := s - p \in P$. Therefore $-d + P = P$. But hereby

$$P = -d + P = -(s - p) + (S - p) = -s + p + S - p = S - s$$

Thus we have $S - s = -d + P = P = S - p$ for any $s \in S$. In particular $S - t = P = S - s$ for any two $s, t \in S$. Now the implication (a) $\implies$ (b) is easy: Since $S - p$ is a sub-module of M and we also know that $S - s = S - p \leq_{\mathsf{m}} M$ is the same set, clearly $S - s \leq_{\mathsf{m}} M$ is a sub-module, too. The converse implication (b) $\implies$ (a) is trivial, as S is non-empty.

(4.117) Example:

(i) If $P \leq_{\mathsf{m}} M$ is a sub-module of M then P is an affine subspace of M. And the dimension of P as a module is precisely the dimension of P as an affine subspace [by taking $s = 0$].

(ii) Conversely any affine subspace $S \subseteq M$ is of the form $S = p + P$ for some $p \in M$ and some sub-module $P \subseteq M$. We will mostly regard the case of a **line** - a 1-dimensional affine space in M

$$S = p + Ru$$

for some $0 \neq u \in R$ or a **plane** in M. The latter is spanned by two (linearly independent) elements $u, v \in M$ and hence is a 2-dimensional affine space in M

$$S = p + Ru + Rv$$

(iii) If $\{ S_i \mid i \in I \}$ is an arbitrary collection of affine spaces $S_i \subseteq M$, then their intersections either empty of another affine space in M

$$\bigcap_{i\in I} S_i \subseteq M \text{ affine space} \iff \bigcap_{i\in I} S_i \neq \emptyset$$

Prob If $S := \bigcap_i S_i$ is empty, then there is nothing to prove. If not we pick up some $p \in S$. As $p \in S \subseteq S_i$ for any $i \in I$ we find that $P_i := S_i - p \leq_{\mathfrak{m}} M$ is a sub-module of M. Let $P := \bigcap_i P_i \leq_{\mathfrak{m}} M$, then we will show: $S = p + P$. As $P \subseteq P_i$ for any $i \in I$ we clearly have $p + P \subseteq p + P_i = S_i$. Conversely if $x \in S$ then $x - p \in S_i - p = P_i$ for any $i \in I$. Thus $x - p \in P$ such that $x \in p + P$. And by $S = p + P$ it is clear that S is an affine space.

Elementary geometry usually starts in the some space $\mathbb{R}^n$ and considers points, lines, line segments, triangles, quadrangles and such. Using set theory we may model all these objects as subsets of the ambient space. E.g. the triangle $T = ABC$ in $\mathbb{R}^n$ is the collection of points in $\mathbb{R}^n$ that lie inside T. We will now formalize these notions: Thereby the triangle $ABC \subseteq \mathbb{R}^n$ will be the convex hull $\mathrm{Ch}\{ A, B, C \}$ of the points A, B, $C \in \mathbb{R}^n$. Generally speaking $A_1A_2 \ldots A_m$ is just another notation for $\mathrm{Ch}\{ A_1, A_2, \ldots, A_m \}$.

(4.118) Definition:
Let V be an $\mathbb{R}$-vector-space, x, $y \in V$ be two points in V and C, $X \subseteq V$ be subsets of V. Then we define the following notions

(i) We denote the **line segment** from x to y (that is the set of points in V starting in x and going straight to y) by $[x, y]$. Formally that is

$$\begin{aligned} [x,y] &:= \{ ax + by \mid a, b \in \mathbb{R}^+,\ a + b = 1 \} \\ &= \{ x + b(y - x) \mid b \in \mathbb{R},\ 0 \leq a \leq 1 \} \end{aligned}$$

(ii) We say that $C \subseteq V$ is a **convex** set, iff for any two points x, $y \in C$ the line from x to y is contained in C. Formally again this is the property

$$\forall\, x,\, y \in C \ :\ [x,y] \subseteq C$$

(iii) For a finite set $X = \{ x_1, \ldots, x_n \} \subseteq V$ we define the **convex hull** of X to be the set of all convex combinations of the elements $x_k \in X$

$$\mathrm{Ch}\{ x_1, \ldots, x_n \} := \left\{ \sum_{k=1}^{n} a_k x_k \;\middle|\; a_k \in \mathbb{R}^+,\ \sum_{k=1}^{n} a_k = 1 \right\}$$

Likewise the **convex hull** of an arbitrary subset $X \subseteq V$ is the set of all convex combinations of any finitely many elements of X

$$\mathrm{Ch}(X) := \left\{ \sum_{k=1}^{n} a_k x_k \;\middle|\; \begin{array}{l} 1 \leq n \in \mathbb{N},\ x_k \in X \\ a_k \in \mathbb{R}^+,\ \sum_{k=1}^{n} a_k = 1 \end{array} \right\}$$

(4.119) Remark:
Examples of convex sets are abundant in elementary geometry: Clearly the empty set $\emptyset \subseteq V$ and any affine space $S \subseteq V$ are convex sets in V. Also any line segment $[x,y] \subseteq V$ is convex. Likewise any triangle, quadrangle and so on are convex sets. In $V = \mathbb{R}^n$ the ball $B_r(m) := \{\, x \in \mathbb{R}^n \mid \|x-m\| \leq r \,\}$ of radius r with center $m \in \mathbb{R}^n$ is convex. This is untrue for the sphere $S_r(m) := \{\, x \in \mathbb{R}^n \mid \|x-m\| = r \,\}$ of radius r with center $m \in \mathbb{R}^n$ however.

(4.120) Proposition: (viz. 950)
If V be an $\mathbb{R}$-vector-space and $X \subseteq V$ is an arbitrary subset of V the following 3 statements are true

(i) The convex hull $\mathrm{Ch}(X) \subseteq V$ of X is a convex set. And if $x \in X$ is any fixed element of X, then we can also write it, as

$$\mathrm{Ch}(X) \;=\; x + \left\{ \sum_{k=1}^{n} a_k(x_k - x) \;\middle|\; \begin{array}{l} 1 \leq n \in \mathbb{N},\ x_k \in X \\ a_k \in \mathbb{R}^+,\ \sum_{k=1}^{n} a_k \leq 1 \end{array} \right\}$$

(ii) If $I \neq \emptyset$ is any index set and for any $i \in I$ we are given some convex set $C_i \subseteq V$, then the intersection of all the C_i is a convex set in V

$$\bigcap_{i \in I} C_i \;\subseteq\; V \text{ is convex}$$

(iii) In particular there is a smallest convex set containing X. It turns out that this is precisely the convex hull of X, that is we have the identity

$$\bigcap \left\{ C \;\middle|\; \begin{array}{l} X \subseteq C \subseteq V, \\ C \text{ is convex} \end{array} \right\} \;=\; \mathrm{Ch}(X)$$

(4.121) Example:
In $\mathbb{R}^n$ the n-dimensional *simplex* is defined to be the convex hull of 0 and the Euclidean basis vectors e_1 to e_n. Intuitively speaking, this is the pyramid attached at 1 at every coordinate axis with apex in 0

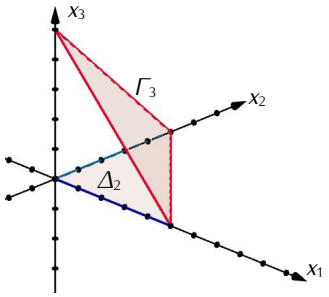
$$\Delta_n \;:=\; \mathrm{Ch}\{\, 0, e_1, \ldots, e_n \,\}$$

As 0 is an element of the generating set of Δ_n we may use (4.120.(i)) (or an immediate comparison) to rewrite this into the following form

$$\Delta_n \;=\; \left\{ (t_1, \ldots, t_n) \in \mathbb{R}^n \;\middle|\; t_k \in \mathbb{R}^+,\ \sum_{k=1}^{n} t_k \leq 1 \right\}$$

We see that Δ_n contains a *facet* Γ_n that is projected $P(\Gamma_n) = \Delta_{n-1}$ onto the $(n-1)$-dimensional simplex $\Delta_{n-1} \subseteq \mathbb{R}^{n-1} \subseteq \mathbb{R}^n$ under the *forgetful map* $P : \mathbb{R}^n \twoheadrightarrow \mathbb{R}^{n-1} : (t_1, t_2, \ldots, t_n) \mapsto (t_2, \ldots, t_n)$

$$\Gamma_n \;=\; \left\{ (t_1, \ldots, t_n) \in \mathbb{R}^n \;\middle|\; t_k \in \mathbb{R}^+,\ \sum_{k=1}^{n} t_k = 1 \right\}$$



(4.122) Proposition: (viz. 951)
Let $1 \leq n \in \mathbb{N}$ and $x \in \mathbb{F}^n$ be a point of n-dimensional space, where $\mathbb{F} \in \{ \mathbb{R}, \mathbb{C} \}$. Then the following statements are true:

(i) If $U \leq_v \mathbb{F}^n$ is a subspace of $\mathbb{F}^n$ then there is a uniquely determined orthogonal projection $p \in U$ of x. And if we choose $\{ g_1, \ldots, g_r, \ldots, g_n \} \subseteq \mathbb{F}^n$ an ONB of $\mathbb{F}^n$ such that $U = \mathrm{Lh}\{ g_1, \ldots, g_r \}$ then we can even compute p by

$$p \;=\; \sum_{k=1}^{r} \langle x \mid g_k \rangle \, g_k$$

(ii) If $S \subseteq \mathbb{F}^n$ is an affine subspace of $\mathbb{F}^n$ then there is a uniquely determined orthogonal projection $p \in S$ of x. And if $s \in S$ is any point in S then we can compute p in the following way: Choose an ONB $\{ g_1, \ldots, g_r, \ldots, g_n \} \subseteq \mathbb{F}^n$ of $\mathbb{F}^n$ such that $S - s = \mathrm{Lh}\{ g_1, \ldots, g_r \}$ then p is given to be

$$p \;=\; s + \sum_{k=1}^{r} \langle x - s \mid g_k \rangle \, g_k$$

(iii) If S is a line in $\mathbb{F}^n$, that is $S = \{ s + au \mid a \in \mathbb{F} \}$ for some points s and $u \in \mathbb{F}^n$ with $u \neq 0$, then the orthogonal projection p of x to S is uniquely determined and can be computed, by

$$p \;=\; s + au \quad \text{where} \quad a \;=\; \frac{\langle x - s, u \rangle}{\|u\|^2}$$

(4.123) Lemma: (viz. 953)
Let $2 \leq n \in \mathbb{N}$ and let $x, y \in \mathbb{R}^n$ be two n-tuples. Then we consider the triangle ABC defined by the points $A = 0 \in R^n$, $B = x$ and $C = y$. Now the angle α in A of ABC satisfies the equation

$$\langle x, y \rangle \;=\; \|x\| \cdot \|y\| \cdot \cos(\alpha)$$

(4.124) Remark:
Lemma (4.123) yields the interpretation of the scalar product as a way to measure the angle α between two vectors x and $y \in \mathbb{R}^n$

$$\cos(\alpha) \;=\; \frac{\langle x, y \rangle}{\|x\| \cdot \|y\|}$$

Note that x and y are perpendicular iff $\cos(\alpha) = 0$ and this is the case iff the scalar product vanishes

$$x \perp y \quad \Longleftrightarrow \quad \langle x, y \rangle \;=\; 0$$

This is formally true for any $x, y \in \mathbb{R}^n$ but we will use this interpretation far more generally by *defining* x and $y \in H$ in a Hilbert space to be perpendicular iff the inner product $\langle x \mid y \rangle = 0$ vanishes. In this sense we can speak of orthogonal functions $f, g : X \to \mathbb{C}$ for example. In the case of the base field $\mathbb{C}$ the interpretation of the angle is a little obscure. But the same reasoning yields the following result: Consider the complex *lines* $\mathbb{C}w$ and $\mathbb{C}z$ where $w, z \in \mathbb{C}^n$. There are two angles α and α' between these lines that sum up to $\alpha + \alpha' = \pi$. Let $\alpha \leq \alpha'$ be the smaller of the two, then

$$|\langle w \mid z \rangle| \;=\; \|w\| \cdot \|z\| \cdot \cos(\alpha)$$

In 2 dimensions - in the plane $\mathbb{R}^2$ - it is clear that for any given direction, defined by $0 \neq x = (x_1, x_2) \in \mathbb{R}^2$ there is precisely one direction $n = (n_1, n_2)$ perpendicular to it. As we have just seen this n has to satisfy the equation

$$x_1 n_1 + x_2 n_2 \;=\; \langle x, n \rangle \;=\; 0$$

This is a homogeneous, linear equation, so the set of solutions $\{ x \}^\perp$ is a subspace of $\mathbb{R}^2$ - not surprisingly, as only the direction of n is determined, not its length. And we immediately see the set of solutions

$$n \;\in\; \{ x \}^\perp \;=\; \mathbb{R} \begin{pmatrix} x_2 \\ -x_1 \end{pmatrix}$$

So what happens in 3 dimensions? Suppose we fix 2 directions by giving a vectors $x, y \in \mathbb{R}^3$. Unless x and y are colinear (= linear dependent) there should be precisely one direction n perpendicular to both x and y. This time n has to satisfy 2 equations, namely

$$\begin{aligned} x_1 n_1 + x_2 n_2 + x_3 n_3 \;&=\; \langle x, n \rangle \;=\; 0 \\ y_1 n_1 + y_2 n_2 + y_3 n_3 \;&=\; \langle y, n \rangle \;=\; 0 \end{aligned}$$

Let us try to solve this system of linear equations, by eliminating a variable: If we multiply the first equation by y_1 and the second equation by x_1 we can eliminate n_1 by subtracting. Then we use the "2d"-trick to guess a solution (n_2, n_3) of this equation with two variables, only

$$\underbrace{(x_2 y_1 - x_1 y_2)}_{-n_3} n_2 + \underbrace{(x_3 y_1 - x_1 y_3)}_{n_2} n_3 \;=\; 0$$

In order to find n_1 we eliminate n_3 by multiplying the first equation with y_3, the second with x_3 and subtracting again. This time we find

$$\underbrace{(x_1 y_3 - x_3 y_1)}_{-n_2} n_1 + \underbrace{(x_2 y_3 - x_3 y_2)}_{n_1} n_2 \;=\; 0$$

We see that our solution for n_2 agrees, so it seems we have stumbled upon something interesting: The direction $\{ x, y \}^\perp$ perpendicular to both x and $y \in \mathbb{R}^3$ seems to be given by

$$n \;\in\; \{ x, y \}^\perp \;=\; \mathbb{R} \begin{pmatrix} x_2 y_3 - x_3 y_2 \\ x_3 y_1 - x_1 y_3 \\ x_1 y_2 - x_2 y_1 \end{pmatrix}$$

(4.125) Definition:
Let $(R,+,\cdot)$ be a commutative ring and consider two triples $x=(x_1,x_2,x_3)$ and $y=(y_1,y_2,y_3)\in R^3$ then we define the **wedge product** (which is more commonly called **cross product**) of x and y by

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \wedge \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} := \begin{pmatrix} x_2y_3 - x_3y_2 \\ x_3y_1 - x_1y_3 \\ x_1y_2 - x_2y_1 \end{pmatrix}$$

The wedge product is a classic construction that has surprisingly many applications. What we are interested in here, is that we may define a plane in $\mathbb{R}^3$ by giving a vector perpendicular to it. But the wedge product may also be used to compute the area of a parallelogram or the volume of a parallelepiped in $\mathbb{R}^3$. So how do we define these objects in vector geometry?

(4.126) Proposition: (viz. 954)
If $(R,+,\cdot)$ is any commutative ring, a, b and $x\in R^3$ such that $a\wedge x=b$, then we find that $\langle a,b\rangle=0$ and

$$\begin{aligned} a_1x &= \begin{pmatrix} 0 \\ b_3 \\ -b_2 \end{pmatrix} + x_1a \\ a_2x &= \begin{pmatrix} -b_3 \\ 0 \\ b_1 \end{pmatrix} + x_2a \\ a_3x &= \begin{pmatrix} b_2 \\ -b_1 \\ 0 \end{pmatrix} + x_3a \end{aligned}$$

Conversely: In case $\langle a,b\rangle=0$ and $a_1\in R^*$ we thereby find that the set of solutions x of the equation $a\wedge x=b$ is the following line in R^3

$$\{\, x\in R^3 \mid a\wedge x=b \,\} = \begin{pmatrix} 0 \\ a_1^{-1}b_3 \\ -a_1^{-1}b_2 \end{pmatrix} + Ra$$

Likewise, if $\langle a,b\rangle=0$ and $a_2\in R^*$ respectively if $a_3\in R^*$ then we find the following analoguos identities

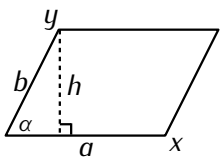
$$\{\, x\in R^3 \mid a\wedge x=b \,\} = \begin{pmatrix} -a_2^{-1}b_3 \\ 0 \\ a_2^{-1}b_1 \end{pmatrix} + Ra$$

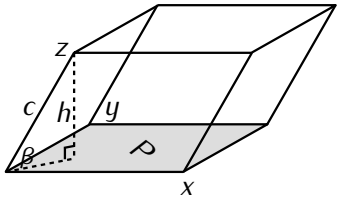
$$\{\, x\in R^3 \mid a\wedge x=b \,\} = \begin{pmatrix} a_3^{-1}b_2 \\ -a_3^{-1}b_1 \\ 0 \end{pmatrix} + Ra$$

(4.127) Definition:
Let V be an $\mathbb{R}$-vector space and $x_1, \ldots, x_k \in V$ be any vectors in V. Then we define the **parallelotope** spanned by the x_i to be the linear hull of the x_i with coefficients $0 \leq a_i \leq 1$ only

$$\mathrm{Ph}\{\, x_1, \ldots, x_n \,\} \;:=\; \left\{ \sum_{i=1}^{k} a_i x_i \mid a_i \in [0,1] \right\}$$

Let us append some elementary geometry: In planar geometry a parallelotope $P = \mathrm{Ph}\{\, x, y \,\}$ (where x, $y \in \mathbb{R}^3$) is called a *parallelogram*. In this case we define the *area* of P as shown in the figure below. And in spatial geometry a parallelotope $Q = \mathrm{Ph}\{\, x, y, z \,\}$ (where x, y, $z \in \mathbb{R}^3$) is called a *parallelepiped*. In this case we define its *volume* as shown in the figure:





$\mathrm{Area}(P) = ah = ab{\cdot}\sin(\alpha)$

$\mathrm{Vol}(Q) = \mathrm{Area}(P){\cdot}h$
$= \mathrm{Area}(P){\cdot}c{\cdot}\sin(\beta)$

(4.128) Proposition: (viz. 955)
If $(R, +, \cdot)$ is a commutative ring and we are given five triples u, v, x, y and $z \in R^3$ then the wedge product satisfies the following properties

(1) $x \wedge x \;=\; 0$

(2) $x \wedge y \;=\; -(y \wedge x)$

(3) $R^3 \times R^3 \to R^3 : (x, y) \mapsto x \wedge y$ is bilinear

(4) $(x \wedge y) \perp x$ and $(x \wedge y) \perp y$

(5) $x \wedge y \;=\; \begin{pmatrix} 0 & -x_3 & x_2 \\ x_3 & 0 & -x_1 \\ -x_2 & x_1 & 0 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$

(6) $\langle x \wedge y, z \rangle \;=\; \det \begin{pmatrix} | & | & | \\ x & y & z \\ | & | & | \end{pmatrix}$

(7) $x \wedge (y \wedge z) \;=\; \langle x, z \rangle\, y - \langle x, y \rangle\, z$

(8) $x \wedge (y \wedge z) + y \wedge (z \wedge x) + z \wedge (x \wedge y) \;=\; 0$

(9) $\langle u \wedge v, x \wedge y \rangle \;=\; \langle u, x \rangle \cdot \langle v, y \rangle - \langle u, y \rangle \cdot \langle v, x \rangle$

(10) $x \wedge y \neq 0 \iff \{\, x, y \,\}$ linear independent

Hereby property (7) is called the *Jacobi* and (9) is called the *Lagrange identity* of the wedge product. And if $A \in \mathrm{mat}_3(R)$ is any matrix, then we have the *transformation formula* (where $\mathrm{cof}(A)$ is the cofactor matrix of A, i.e. the matrix of (2×2)-minors of A)

$$(Ax) \wedge (Ay) \;=\; \mathrm{cof}(A)(x \wedge y)$$

Now, if $R = \mathbb{R}$ then the norm of the cross product is precisely the area of the parallelogram spanned by x and y. That is if α is the angle between theg vectors x and y then we get

$$\|x \wedge y\| = \mathrm{Area}\big(\mathrm{Ph}\{\, x, y \,\}\big) = \|x\| \cdot \|y\| \cdot \sin(\alpha)$$

Likewise, if x, y and $z \in \mathbb{R}^3$ then the volume of the *parallelepiped* spanned by x, y and z can be computed using the *triple product* of x, y and z

$$\langle x \wedge y, z \rangle \;=\; \mathrm{Vol}\big(\mathrm{Ph}\{\, x, y, z \,\}\big)$$

(4.129) Remark: $(\diamondsuit)$
In the definition of the area of a parallelogram or the volume of a parallelepiped we strongly appealed to the intuition of the reader. There is an entire mathematical discipline called *measure theory* dedicated to the problem of defining the volume of geometric objects in $\mathbb{R}^n$. The best answer to this problem is the *Lebesgue-measure* and it turns out, not all subsets $X \subseteq \mathbb{R}^n$ can be assigned a reasonable volume. There are X that are just too weird, to do so (e.g. the *Banach-Tarski-Paradox*).
A very readable introduction to the topic is the first chapter of [Bauer, Maß- und Integrationstheorie]. Theorem (8.4) in this textbook states that for any $\mathbb{R}$-linear $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ and any Borel set $A \subseteq \mathbb{R}^n$ [that is a set that can be assigned a reasonable volume] the Lebesgue-measure λ satisfies

$$\lambda\big(\varphi(A)\big) \;=\; \det(\varphi) \cdot \lambda(A)$$

In this light the volume formula above is just a special case of this: Define $\varphi : \mathbb{R}^3 \to \mathbb{R}^3$ by $\varphi(e_1) := x$, $\varphi(e_2) := y$ and $\varphi(e_3) := z$. Take $C := [0,1]^3$ the standard cube in $\mathbb{R}^3$. It stands to reason, that λ has been defined in such a way as $\lambda(C) = 1$. Then $Q := \varphi(C) = \mathrm{Ph}\{\, x, y, z \,\}$ and we get

$$\mathrm{Vol}(Q) \;=\; \lambda(Q) \;=\; \det(\varphi) \cdot \lambda(C) \;=\; \det \begin{pmatrix} | & | & | \\ x & y & z \\ | & | & | \end{pmatrix} \;=\; \langle x \wedge y, z \rangle$$

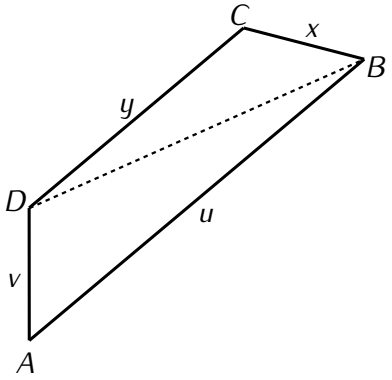
(4.130) Example: (viz. 959)
Consider any four points A, B, C and $D \in \mathbb{R}^3$ in three-dimensional space. We say that their convex hull $T := ABCD = \mathrm{Ch}\{\, A, B, C, D \,\}$ is a *trapezoid*, iff these points form a quadrangle in $\mathbb{R}^3$ such that two sides of the quadrangle are parallel. E.g. we may assume the property

$$C - D \;=\; t(B - A)$$

for some $t \in \mathbb{R}^+$. In this case these four points lie in a plane in $\mathbb{R}^3$ as $C = A + t(B - A) + (D - A)$. And the area of T can be computed using the wedge product in the following way

$$\text{Area}(T) \;=\; \frac{1}{2} \left\| \Big((B - A) + (C - D) \Big) \wedge (C - A) \right\|$$

This is due to the fact, that we can decompose the trapezoid $T = ABCD$ into two triangles ABD and BCD and compute their areas using the wedge product of the edges $u = B - A$ and $v = D - A$ for ABD, resp. $x = C - B$ and $y = D - C$ for BCD



(4.131) Theorem: (viz. 959)
Let u and $v \in \mathbb{R}^3$ be any two linearly independent vectors in $\mathbb{R}^3$. Also let $s \in \mathbb{R}^3$ be any point, then we regard the following plane in $\mathbb{R}^3$

$$S \;:=\; s + \text{Lh}\{\, u, v \,\} \;\subseteq\; \mathbb{R}^3$$

If we let $n := u \wedge v$ and $h := \langle n, s \rangle$, then S is the set of solutions x of the linear equation $\langle n, x \rangle = h$, formally that is: S is given to be

$$S \;=\; \big\{\, x \in \mathbb{R}^3 \mid \langle u \wedge v, x \rangle = \langle u \wedge v, s \rangle \,\big\}$$

(4.132) Remark:
The above theorem tells us that there are two ways to define a plane S in $\mathbb{R}^3$: First of all we can give a *parametrization* of S, that is we choose a starting point $s \in \mathbb{R}^3$ and two directions u, $v \in \mathbb{R}^3$ (note that $\{\, u, v \,\}$ has to be linearly independent, to span a plane) and take S to be the set

$$S \;:=\; s + \mathbb{R}u + \mathbb{R}v \;\subseteq\; \mathbb{R}^3$$

Secondly we can describe S *implicitly* by giving an equation $f(x) = 0$ such that S is comprised of all the points $x \in \mathbb{R}^3$ that satisfy the defining equation f. In this case we pick up a perpendicular direction $n = (n_1, n_2, n_3) \in \mathbb{R}^3$ (which should be non-zero $n \neq 0$ to define a plane) and some scalar $h \in \mathbb{R}$ and take $f(x) = \langle n, x \rangle - h$. That is

$$H \;:=\; \big\{\, x \in \mathbb{R}^3 \mid n_1 x_1 + n_2 x_2 + n_3 x_3 = h \,\big\}$$

By the theorem above, we can take $n := u \wedge v$ and $h := \langle n, s \rangle$ then these planes agree $H = S$. Conversely, if we are given H in implicit form it also is easy to find a parametrization S: As $n \neq 0$ there is some $n_i \neq 0$, say $n_3 \neq 0$. We need u, v and $s \in \mathbb{R}^3$ such that $\langle n, u \rangle = 0$, $\langle n, v \rangle = 0$ and $\langle n, s \rangle = 0$. But these are easy to find: For $n_3 \neq 0$ let

$$\begin{aligned} u &:= (n_3, 0, -n_1) \\ v &:= (0, n_3, -n_2) \\ s &:= (0, 0, h/n_3) \end{aligned}$$

Then it is easy to see that $u \wedge v = n_3 n$ and $\langle u \wedge v, s \rangle = n_3 \langle n, s \rangle = n_3 h$. Thus for any $x \in \mathbb{R}^3$ we have $\langle u \wedge v, x \rangle = n_3 \langle n, x \rangle$ and $\langle u \wedge v, s \rangle = n_3 h$, such that $\langle u \wedge v, x \rangle = \langle u \wedge v, s \rangle$ becomes equivalent to $\langle n, x \rangle = h$. By the theorem above this results in $H = S$ such that we can switch freely between a parametrization and an implicit description of a plane in $\mathbb{R}^3$, as needed.

This can even be generalized to arbitrary dimensions $d \geq 2$. Given any $n = (n_1, n_2, \ldots, n_d) \in \mathbb{R}^d$ such that $n \neq 0$ and $h \in \mathbb{R}$ the set of solutions of the equation $\langle n, x \rangle = h$ is said to be a *hyperplane* in $\mathbb{R}^d$

$$H := \left\{ x \in \mathbb{R}^d \mid \langle n, x \rangle = h \right\}$$

This means that the dimension of H is one less, than the dimension of the ambient space $\mathbb{R}^d$. That is we need $d - 1$ vectors $u_1, \ldots, u_{d-1} \in \mathbb{R}^d$ and a starting point $s \in \mathbb{R}^d$ to span H. So let's take a look at

$$S := s + \mathbb{R}u_1 + \cdots + \mathbb{R}u_{d-1} \subseteq \mathbb{R}^d$$

Note that thereby $\{ u_1, \ldots, u_{d-1} \}$ has to be linearly independent of course. So what's the relation between these two descriptions? If $n_d \neq 0$ then it is easy to give the u_i and s again:

$$\begin{aligned} u_i &:= n_d \, e_i - n_i \, e_d \\ s &:= (h/n_d) \, e_d \end{aligned}$$

(where $i \in 1 \ldots d-1$ and $\{ e_1, \ldots, e_d \}$ is the Euclidean basis of $\mathbb{R}^d$). Then $\langle n, u_i \rangle = 0$ and $\langle n, s \rangle = h$ such that $S \subseteq H$. But as both have the same dimension this means $S = H$. The converse direction requires some more effort however: Regard the matrix $U \in \mathrm{mat}_{(d-1),d}(\mathbb{R})$ that has the rows $\mathrm{row}_i(U) = u_i$. That is $Ux = (\langle u_1, x \rangle, \ldots, \langle u_{d-1}, x \rangle)$. As the u_i are linearly independent it has row-rank $d - 1$ and hence $x \mapsto Ux$ is surjective. By the dimension formula this means that its kernel is 1-dimensional, that is $\mathrm{kn}(U) = \mathbb{R}n$ for some $n \neq 0$. We can find this n using the Gaussian elimination algorithm. Thus if we let $h := \langle n, s \rangle$ again then we have found n and h such that $H = S$. The computation of n is precisely what the wedge product does in three dimensions.

Let us append a final comment on this, without going into details: The equivalence of an explicit parametrization S and an implicit description H remains true in the much more general setting of differential geometry:

An r-dimensional *submanifold* of $\mathbb{R}^d$ is a subset $M \subseteq \mathbb{R}^d$ that can locally be parametrisized by (differentiable) maps $\varphi : D \subseteq \mathbb{R}^r \hookrightarrow M \subseteq \mathbb{R}^d$. And it turns out that this is equivalent to saying, that locally M can be described as the set of roots $M \cap U = \{ x \in U \mid f(x) = 0 \}$ of some (differentiable) function $f : U \subseteq \mathbb{R}^d \to \mathbb{R}$. But this is an entirely different story.

(4.133) Remark:
An elementary problem in geometry is the following: We are given a point $x = (x_1, x_2) \in \mathbb{R}^2$ and want to rotate it by the angle $\varphi \in [0, 2\pi]$ around the center of rotation $c = (c_1, c_2) \in \mathbb{R}^2$. Which coordinates $x' \in \mathbb{R}^2$ is x mapped to? The answer is rather simple

$$x' \;=\; \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} + \begin{pmatrix} \cos(\varphi & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix} \begin{pmatrix} c_1 - x_1 \\ c_2 - x_2 \end{pmatrix}$$

This can also be expressed in terms of complex numbers: The multiplication by $e^{i\varphi} = \cos(\varphi) + i\sin(\varphi)$ rotates $z \in \mathbb{C}$ by the angle φ around $0 \in \mathbb{C}$. Thus if $c = c_1 + ic_2$ and $x = x_1 + ix_2$ then

$$x' \;=\; c + e^{i\varphi} \cdot (x - c)$$

(4.134) Remark:
Rotations in spatial geometry require some more information: First of all we need to fix a center $c \in \mathbb{R}^3$ of rotation and a rotation axis, which is defined by some vector $n \in \mathbb{R}^3$ with $n \neq 0$. Now we want to rotate a point $x \in \mathbb{R}^3$ by the angle $\varphi \in [0, 2\pi]$. To do this we need an orthonormal basis $\{ u_1, u_2, u_3 \}$ of $\mathbb{R}^3$ in which the rotation axis is a coordinate axis. If $n_1 \neq 0$ this can be achieved by

$$u_1 \;=\; \frac{1}{a} \begin{pmatrix} -n_2 \\ n_1 \\ 0 \end{pmatrix}, \;\; u_2 \;=\; \frac{1}{ab} \begin{pmatrix} -n_1 n_3 \\ -n_2 n_3 \\ n_1^2 + n_2^2 \end{pmatrix}, \;\; u_3 \;=\; \frac{1}{b} \begin{pmatrix} n_1 \\ n_2 \\ n_3 \end{pmatrix}$$

where $a := \sqrt{n_1^2 + n_2^2}$ and $b := \sqrt{n_1^2 + n_2^2 + n_3^2}$. Then u_1 and u_2 are a basis of the plane E defined by $\langle x, n \rangle = 0$ and u_3 is perpendicular to E. In case $n_1 = 0$ the same is true for

$$u_1 \;=\; \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \;\; u_2 \;=\; \frac{1}{b} \begin{pmatrix} 0 \\ n_3 \\ -n_2 \end{pmatrix}, \;\; u_3 \;=\; \frac{1}{b} \begin{pmatrix} 0 \\ n_2 \\ n_3 \end{pmatrix}$$

In any case, all we need to do is rotate to find a basis representation of $x - c$ in the basis $\{ u_1, u_2, u_3 \}$ and rotate the first two coefficients as we did in $\mathbb{R}^2$. As $\{ u_1, u_2, u_3 \}$ is an ONB the basis representation is easy to find by evaluating scalar products: If $r_k := \langle x - c, u_k \rangle$ then $x - c = r_1 u_1 + r_2 u_2 + r_3 u_3$ and thereby x is rotated onto

$$x' \;=\; c + \Big(r_1 \cos(\varphi) - r_2 \sin(\varphi) \Big) u_1 + \Big(r_1 \sin(\varphi) + r_2 \cos(\varphi) \Big) u_2 + r_3 u_3$$

Analogous to the planar case, there is a way of expressing this using quaternions: First of all we employ the usual embedding $\mathbb{R}^3 \hookrightarrow \mathbb{H}$ that takes $x = (x_1, x_2, x_3) \mapsto ix_1 + jx_2 + kx_3$ that is $x \in \mathbb{R}^3$ is mapped to a quaternion with real part 0. Then we encode n and φ in $q \in \mathbb{H}$ by

$$q \;:=\; \cos\left(\frac{\varphi}{2}\right) + \sin\left(\frac{\varphi}{2}\right) \|n\|^{-1} \left(in_1 + jn_2 + kn_3\right)$$

Then $x \in \mathbb{R}^3$ is mapped onto the point $x' \in \mathbb{R}^3$ under rotation, where x' can be computed using the following conjugation with q

$$x' \;=\; c + \mathrm{im}\Big(q(x-c)q^{-1}\Big)$$

(4.135) Remark: $(\diamondsuit)$
As we have just argued the plane perpendicular to $n = (n_1, n_2, n_3) \in \mathbb{R}^3$ (where $n \neq 0$) that contains the point $s = (s_1, s_2, s_3) \in \mathbb{R}^3$ is defined by the equation

$$n_1x_1 + n_2x_2 + n_3x_3 \;=\; n_1s_1 + n_2s_2 + n_3s_3$$

Thereby "defined by" clearly means, that it consists of all the solutions $x = (x_1, x_2, x_3) \in \mathbb{R}^3$ that satisfy this equation. Likewise we have seen that the equation

$$\big(x_1 - c_1\big)^2 + \big(x_2 - c_2\big)^2 + \big(x_3 - c_3\big)^2 \;=\; r^2$$

defines a sphere of radius $r > 0$ around the center $c = (c_1, c_2, c_3) \in \mathbb{R}^3$ (in the same sense). Intersecting to planes we get a line. Algebraically speaking that is: We only allow those $x \in \mathbb{R}^3$ that satisfy both equations of the respective planes. Likewise the intersection of a sphere and a plane is a circle in space. Thus the intersection of geometric objects yields another geometric object (that may be empty).
Note that the equations we used here are polynomial, this is the restriction we use in algebraic geometry. So generally speaking a geometric object $X \subseteq \mathbb{R}^n$ in this sense is the common zero-locus of a set of polynomials $F \subseteq \mathbb{R}[t_1, \ldots, t_n]$ (it is called an *affine variety* over $\mathbb{R}$ or any other field). That is

$$X \;=\; \mathbb{V}(F) \;:=\; \{\, x \in \mathbb{R}^n \mid \forall\, f \in F \,:\, f(x) = 0 \,\}$$

The mathematical field of algebraic geometry now tries to glean geometric properties of X by studying the algebraic properties of the ring $\mathcal{O}(X)$ of polynomial functions on X. That is $p \in \mathcal{O}(X)$ is a so-called *regular* function $p : X \to \mathbb{R}$ on X, if indeed there is a polynomial $f \in \mathbb{R}[t_1, \ldots, t_n]$ such that $p(x) = f(x)$ for any $x \in X$. So let $q \in \mathcal{O}(X)$ be another regular function on X, induced by the polynomial $g \in \mathbb{R}[t_1, \ldots, t_n]$. When are p and q identical? Clearly iff

$$\begin{aligned} p = q \;&\iff\; \forall\, x \in X \,:\, f(x) \,=\, g(x) \\ &\iff\; f - g \,\in\, \{\, h \in \mathbb{R}[t_1, \ldots, t_n] \mid \forall\, x \in X : h(x) = 0 \,\} \end{aligned}$$

It is plain to see that the set $\mathbb{I}(X) := \{\, h \in \mathbb{R}[t_1, \ldots, t_n] \mid \forall\, x \in X : h(x) = 0 \,\}$ is an ideal in the polynomial ring $\mathbb{R}[t_1, \ldots, t_n]$. It is called the *vanishing ideal* of X. So the boon here is, that the ring of regular functions is nothing but a residue of the polynomial ring

$$\mathbb{R}[t_1, \ldots, t_n] \Big/ \mathbb{I}(X) \;\cong_{\mathrm{r}}\; \mathcal{O}(X) \;:\; f + \mathbb{I}(X) \;\mapsto\; \big(x \mapsto f(x)\big)$$

4.9 Linear Optimization

Chapter 5

Structure Theorems

5.1 Primary Decomposition

In section 2.8 we introduced the notion of *primary ideals* and the *primary decomposition* of an ideal $\mathfrak{a} \trianglelefteq_\mathfrak{i} R$. The theory culminated in the theorem of Lasker-Noether: If R is a noetherian ring and $\mathfrak{a} \neq R$ is a proper ideal, then $\mathfrak{a}$ admits a minimal primary decomposition. That is there are some primary ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_k \in \operatorname{Spri}(R)$ such that $\mathfrak{a}$ is the intersection of the $\mathfrak{a}_i$ but not of a subset of these. That is for any $j \in 1 \ldots k$ we get

$$\begin{aligned} \mathfrak{a} &= \bigcap_{i=1}^{k} \mathfrak{a}_i \\ \mathfrak{a} &\neq \bigcap_{i \neq j} \mathfrak{a}_i \end{aligned}$$

Also, if we denote $\mathfrak{p}_i := \sqrt{\mathfrak{a}_i}$ and $\operatorname{ass}(\mathfrak{a}) := \{\, \mathfrak{p}_1, \ldots, \mathfrak{p}_k \,\}$, then $\mathfrak{p}_i \in \operatorname{Spec}(R)$, as the $\mathfrak{a}_i$ are primary ideals. And we can choose the $\mathfrak{a}_i$ in such a way, that the $\mathfrak{p}_i$ are pairwise distinct [all we have to do, is to take the intersection of all the $\mathfrak{a}_i$ that belong to the same associated ideal $\mathfrak{p} \in \operatorname{ass}(\mathfrak{a})$, then the resulting intersections are a new set of $\mathfrak{a}_i$ that satisfy the properties above and]

$$\forall\, i, j \in 1 \ldots k \;:\; \mathfrak{p}_i = \mathfrak{p}_j \implies i = j$$

And in this case the following information on $\mathfrak{a}$ is uniquely determined: (1) the number k of ideals in the primary decomposition, (2) the set $\operatorname{ass}(\mathfrak{a})$ of associate prime ideals and (3) the so-called *isolated components* of $\mathfrak{a}$. These are the primary ideals $\mathfrak{a}_i$ for which $\mathfrak{p}_i$ is a minimal element of $\operatorname{ass}(\mathfrak{a})$. Formally that is: The following set is uniquely determined, as well

$$\operatorname{iso}(\mathfrak{a}) := \left\{ \mathfrak{a}_j \;\middle|\; \forall\, i \in 1 \ldots k \;:\; \mathfrak{p}_i \subseteq \mathfrak{p}_j \implies \mathfrak{p}_i = \mathfrak{p}_j \right\}$$

In fact the minimal elements of $\operatorname{ass}(\mathfrak{a})$ are precisely the prime ideals that are minimal over $\mathfrak{a}$. Therefore the set of isolated components of $\mathfrak{a}$ can also be expressed in the following way

$$\operatorname{iso}(\mathfrak{a}) = \left\{ \mathfrak{a}_j \;\middle|\; \mathfrak{p}_j \in \{\, \mathfrak{q} \in \operatorname{Spec}(R) \mid \mathfrak{a} \subseteq \mathfrak{q} \,\}_* \right\}$$

Note that ideals $\mathfrak{a} \trianglelefteq_\mathfrak{i} R$ are nothing but modules over R. So in this section we will generalize the Lasker-Noether-decomposition to the case of modules over a commutative ring R. In order to do so we

will have to introduce the notion of a prime ideal *associated* to a module M. This decomposition will be used to prove the uniqueness of the invariant factors, but the notion of an associated prime ideal is of importance in its own right.

(5.1) Definition:
Let $(R,+,\cdot)$ be a commutative ring, M be an R-module, $L \leq_{\mathfrak{m}} M$ a sub-module of M and consider some $p \in R$. Then we define the **p-primary** component $L(p)$ of L to be the subset of elements of L that are annihilated by some power of a, formally that is

$$L(p) \;:=\; \{\, x \in L \mid \exists\, n \in \mathbb{N} : p^n x = 0 \,\}$$

And we say that p **annihilates** L, iff $L = L(p)$, that is iff for any $x \in L$ there is some $n \in \mathbb{N}$ such that $p^n x = 0$. Note that different x may require different powers n of p.

(5.2) Remark:
In mathematical literature there are an awful lot of ambiguities concerning this topic. The primary component $L(p)$ is often denoted L_p but this can be confused with the localizations $\{1, p, p^2, \dots\}^{-1} L$ or even $(R \setminus pR)^{-1}R$. Hence we chose a different notation. Also some textbooks say that L is *primary* if $L = L(p)$ for some prime element $p \in R$. This notion only is suitable over PIDs however. Hence we will reserve the word *primary* for a more general notion, that has to be introduced yet and will work fine over general noetherian rings R. This notion will be taken from Bourbaki.

(5.3) Proposition: (viz. 1154)
Let $(R,+,\cdot)$ be a commutative ring, fix some $p \in R$, let M be an R-module and consider $L \leq_{\mathfrak{m}} M$ a sub-module of M. Then the following statements are true

(i) Clearly for any $a \in R$ we have $L(p) \subseteq L(ap)$.

(ii) The p-primary component $L(p)$ of L is a sub-module of L, formally: $L(p) \leq_{\mathfrak{m}} L \leq_{\mathfrak{m}} M$.

(iii) We find that p annihilates M if and only if p annihilates both L and the residue module M/L. That is the following two statements are equivalent:

 (a) p annihilates M

 (b) p annihilates both, L and M/L

(iv) If p annihilates finitely many sub-modules $L_1, \dots, L_r \leq_{\mathfrak{m}} M$ [that is if for any $i \in 1 \dots r$ we have $L_i(p) = L_i$], then p also annihilates their sum $L_1 + \cdots + L_r \leq_{\mathfrak{m}} M$, too.

(v) If N is another R-module and $\varphi : M \to N$ is a homomorphism of R-modules, then for any $p \in R$ we have the inclusion $\varphi(M(p)) \subseteq N(p)$. And if φ is injective we also have $\varphi^{-1}(N(p)) \subseteq M(p)$.

(5.4) Example: (viz. 1153)
Let $(R,+,\cdot)$ be an UFD, $s \in \mathbb{N}$ and for any $j \in 1\ldots s$ let $p(j) \in R$ be a prime element of R, such that the $p(j)$ are non-associated, that is for any $j, k \in 1\ldots s$ we suppose $p(j) \approx q(k) \implies j = k$. Also for any $j \in 1\ldots s$ let $1 \leq I(j) \in \mathbb{N}$ and for $i \in 1\ldots I(j)$ let $1 \geq n(i,j) \in \mathbb{N}$. Then we regard the R-module

$$M \;:=\; \bigoplus_{j=1}^{s} \bigoplus_{i=1}^{I(j)} R \Big/ p(j)^{n(i,j)} R$$

Note that the torsion part of any finitely generated module over a PID can be written in this *invariant factor form*, as we will see in section 5.2. Then for any prime $q \in R$ we either have $M(q) = 0$ iff $q \approx p(j)$ is untrue for all $j \in 1\ldots s$ and conversely, if $q \approx p(k)$ for some $k \in 1\ldots s$, then

$$M(q) \;=\; \bigoplus_{i=1}^{I(k)} R \Big/ p(k)^{n(i,k)} R$$

(5.5) Definition:
Let $(R,+,\cdot)$ be a commutative ring and M be an R-module. Recall that for any $x \in M$ we defined the **annihilator** of x to be the ideal of all $a \in R$ such that $ax = 0$, that is

$$\operatorname{ann}_R(x) \;:=\; \operatorname{kn}\big(R \to M \;:\; a \mapsto ax\big) \quad \trianglelefteq_{\mathrm{i}} \quad R$$

(i) The set of all proper annihilators of M is denoted by $\operatorname{Anns}_R(M)$. The set of annihilator ideals, that also are prime ideals called the **annihilator spectrum** of M and is denoted, by $\operatorname{Sann}_R(M)$. That is

$$\begin{aligned} \operatorname{Anns}_R(M) &:= \{\, \operatorname{ann}_R(x) \mid 0 \neq x \in M \,\} \quad \subseteq \quad \operatorname{Ideal}(R) \\ \operatorname{Sann}_R(M) &:= \operatorname{Anns}_R(M) \cap \operatorname{Spec}(R) \end{aligned}$$

If the base ring R is understood, we will usually omit the index R in all these notations and just write $\operatorname{ann}(x)$, $\operatorname{Anns}(M)$ and $\operatorname{Sann}(M)$ instead.

(ii) A prime annihilator ideal $\mathfrak{p} \in \operatorname{Sann}(M)$ of M is said to be an **isolated prime** iff it is minimal in $\operatorname{Sann}(M)$, that is iff for any $\mathfrak{q} \in \operatorname{Sann}(M)$ we have the implication

$$\mathfrak{q} \subseteq \mathfrak{p} \quad\Longrightarrow\quad \mathfrak{q} = \mathfrak{p}$$

And we denote the set of all isolated primes of M by $\operatorname{Sann}(M)_*$. A prime annihilator ideal $\mathfrak{p} \in \operatorname{Sann}(M)$ of M that is *not* minimal is said to be an **embedded prime** of M.

(iii) Finally we define the **support** of M to be the set of prime ideals of R that contain an annihilator $\operatorname{ann}(x)$ of some element $x \in M$, formally that is the following set

$$\operatorname{Supp}(M) \;:=\; \{\, \mathfrak{p} \in \operatorname{Spec}(R) \mid \exists\, x \in M \;:\; \operatorname{ann}(x) \subseteq \mathfrak{p} \,\}$$

(5.6) Example: (viz. 1154)

(i) If $(R,+,\cdot)$ is an integral domain and $M \leq_{\mathrm{m}} R$ is a non-zero sub-module (i.e. ideal) of R, then the R-module M has a single annihilator ideal: the zero-ideal 0. That is we get

$$\mathrm{Anns}_R(M) \;=\; \mathrm{Sann}_R(M) \;=\; \{0\}$$

(ii) More generally: If $(R,+,\cdot)$ is a non-zero, commutative ring and M is a *torsion-free* R-module, which is $0 = \mathrm{tor}(M) = \{\, x \in M \mid \exists\, a \in R : a \neq 0 \text{ and } ax = 0 \,\}$, then we distinguish two cases:

$$\mathrm{Sann}(M) \;=\; \begin{cases} \{0\} & \text{if } M \neq 0 \text{ and } R \text{ is an integral domain} \\ \emptyset & \text{if } M = 0 \text{ or } R \text{ is not an integral domain} \end{cases}$$

(iii) If $(R,+,\cdot)$ is a commutative ring and M a simple, non-zero module [i.e. $P \leq_{\mathrm{m}} M$ implies $P = 0$ or $P = M$], then $\mathrm{ann}(M) = \{\, a \in R \mid \forall\, x \in M : ax = 0 \,\}$ is a maximal ideal and this ideal is the one and only annihilator ideal of M. That is we get

$$\mathrm{Anns}_R(M) \;=\; \mathrm{Sann}_R(M) \;=\; \{\, \mathrm{ann}(M) \,\}$$

(iv) If $(R,+,\cdot)$ is a commutative ring and $\mathfrak{p} \in \mathrm{Spec}(R)$ is a prime ideal of R then $\mathfrak{p}$ is the one and only annihilator of $R/\mathfrak{p}$ considered as an R-module. Formally that is

$$\mathrm{Anns}_R\left(R\Big/\mathfrak{p}\right) \;=\; \mathrm{Sann}_R\left(R\Big/\mathfrak{p}\right) \;=\; \{\, \mathfrak{p} \,\}$$

Nota Thereby $\mathfrak{a} \in \mathrm{Anns}_R(R/\mathfrak{a})$ is true for any proper ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$, $\mathfrak{a} \neq R$ of R, but for the converse inclusion the property $ab \in \mathfrak{p},\ b \notin \mathfrak{p} \implies a \in \mathfrak{p}$ of a prime ideal is required.

(v) Consider any commutative ring $(R,+,\cdot)$ and any ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ and recall the notation $\mathbb{V}(\mathfrak{a})$ for the set of prime ideals containing $\mathfrak{a}$, i.e. $\mathbb{V}(\mathfrak{a}) := \{\, \mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{a} \subseteq \mathfrak{p} \,\}$. If we now regard $R/\mathfrak{a}$ as an R-module, then we obtain the identity

$$\mathrm{Supp}_R\left(R\Big/\mathfrak{a}\right) \;=\; \mathbb{V}(\mathfrak{a})$$

Nota in particular for $\mathfrak{a} = 0$ this yields: If we regard R as an R-module, then every prime ideal of R already is contained in the support $\mathrm{Supp}_R(R) = \mathrm{Spec}(R)$ of R.

(5.7) Lemma: (viz. 1155)
Let $(R,+,\cdot)$ be any commutative ring and M be an R-module, then the following statements are true:

(i) If N is another R-module, $\iota : M \to N$ a monomorphism of R-modules and $x \in M$, then we find that $\mathrm{ann}(\iota(x)) = \mathrm{ann}(x) \trianglelefteq_{\mathrm{i}} R$. In particular this yields the following inclusions

$$\begin{aligned} \mathrm{Anns}_R(M) &\subseteq \mathrm{Anns}_R(N) \\ \mathrm{Sann}_R(M) &\subseteq \mathrm{Sann}_R(N) \\ \mathrm{Supp}_R(M) &\subseteq \mathrm{Supp}_R(N) \end{aligned}$$

Nota In particular, if $M \cong_{\mathsf{m}} N$ are isomorphic, then the above inclusions even are equalities. In other words: Isomorphic modules share the same support and annihilator spectra.

(ii) If $\mathfrak{p} \in \operatorname{Spec}(R)$ is a prime ideal of R and $x \in M$ an element of M, then $\mathfrak{p}$ is the annihilator of x if and only if there is an isomorphism of R-modules between $R/\mathfrak{p}$ and $Rx \leq_{\mathsf{m}} M$. Formally

$$\mathfrak{p} = \operatorname{ann}(x) \iff {}^{R}\!\Big/_{\mathfrak{p}} \cong_{\mathsf{m}} Rx$$

Nota Thereby for any annihilator $\mathfrak{a} = \operatorname{ann}(x) \trianglelefteq_{\mathsf{i}} R$ we obtain the isomorphism $R/\mathfrak{a} \xrightarrow{\sim} Rx : a \mapsto ax$ of R-modules, but for the converse implication we require a prime ideal $\mathfrak{p}$ of R.

(iii) Recall the definition of the *annihilator* $\operatorname{ann}(M) = \{\, a \in R \mid \forall\, x \in M : ax = 0 \,\}$ of M and for some $\mathfrak{a} \subseteq R$ the notation $\mathbb{V}(\mathfrak{a}) = \{\, \mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{a} \subseteq \mathfrak{p} \,\}$. Then the following subsets of the spectrum of R are equal and this subset is called the *support* $\operatorname{Supp}(M)$ of M

$$\begin{aligned}\operatorname{Supp}(M) &= \mathbb{V}\big(\operatorname{ann}(M)\big)\\ &= \{\, \mathfrak{p} \in \operatorname{Spec}(R) \mid M_{\mathfrak{p}} \neq 0 \,\}\\ &= \{\, \mathfrak{p} \in \operatorname{Spec}(R) \mid \exists\, x \in M \,:\, \operatorname{ann}(x) \subseteq \mathfrak{p} \,\}\end{aligned}$$

(iv) Recall the definition $\operatorname{zd}(M) := \{\, a \in R \mid \exists\, x \in M : x \neq 0 \text{ and } ax = 0 \,\}$ of the set of *zero-divisors* of M. This set is the union of all annihilator ideals of M, in formal terms

$$\bigcup \operatorname{Anns}(M) = \operatorname{zd}(M)$$

(v) If $\mathfrak{a} \in \operatorname{Anns}(M)$ is a maximal annihilator ideal [that is for any $\mathfrak{b} \in \operatorname{Anns}(M)$ with $\mathfrak{a} \subseteq \mathfrak{b}$ we already get $\mathfrak{a} = \mathfrak{b}$] then $\mathfrak{a}$ already is a prime ideal and hence $\mathfrak{a} \in \operatorname{Sann}(M)$. Formally this is

$$\Big(\operatorname{Anns}(M)\Big)^{*} \subseteq \operatorname{Sann}(M)$$

(5.8) Proposition: (viz. 1156)
Let $(R, +, \cdot)$ be a commutative ring and M be an R-module. Then we find the following statements concerning the annihilator spectrum of M

(i) If $P \leq_{\mathsf{m}} M$ is a sub-module of M, then the annihilator spectrum of M is contained in the annihilator spectrum of P and M/P, that is

$$\operatorname{Sann}(P) \subseteq \operatorname{Sann}(M) \subseteq \operatorname{Sann}(P) \cup \operatorname{Sann}\Big({}^{M}\!\Big/_{P}\Big)$$

More generally: If $0 \to L \to M \to N \to 0$ is an exact chain of R-modules then we obtain the following inclusions of the annihilator spectra

$$\operatorname{Sann}(L) \subseteq \operatorname{Sann}(M) \subseteq \operatorname{Sann}(L) \cup \operatorname{Sann}(N)$$

(ii) Let $P_i \leq_{\mathsf{m}} M$ be an arbitrary ($i \in I$) family of sub-modules of M that cover M, i.e. $M = \bigcup_i P_i$. Then the annihilator spectrum of M is the union of the of all the annihilator spectra of the P_i

$$\mathsf{Sann}(M) \;=\; \bigcup_{i \in I} \mathsf{Sann}(P_i)$$

(iii) Let $P_i \leq_{\mathsf{m}} M$ be an arbitrary ($i \in I$) family of sub-modules of M such that $\bigcap_i P_i = 0$. Then the annihilator spectrum of M is contained in the union of the of all the annihilator spectra of M/P_i

$$\mathsf{Sann}(M) \;\subseteq\; \bigcup_{i \in I} \mathsf{Sann}\left(M \Big/ P_i\right)$$

(iv) Let M_i be an arbitrary ($i \in I$) family of R-modules M_i. Then the annihilator spectrum of the direct sum of the M_i is the union of all the annihilator spectra of the M_i

$$\mathsf{Sann}\left(\bigoplus_{i \in I} M_i\right) \;=\; \bigcup_{i \in I} \mathsf{Sann}(M_i)$$

(v) If $\mathfrak{p} \in \mathsf{Spec}(R)$ is a prime ideal of R, then $\mathfrak{p}$ is in the annihilator spectrum of M if and only if there is a monomorphism ι of R-modules, that maps $R/\mathfrak{p}$ into M, that is

$$\mathfrak{p} \in \mathsf{Sann}(M) \iff \exists\, \iota : R \Big/ \mathfrak{p} \hookrightarrow M$$

(vi) If R is a non-zero, noetherian ring, then the annihilator spectrum of M is empty, if and only if M is the zero module, that is

$$\mathsf{Sann}(M) = \emptyset \iff M = 0$$

(vii) Recall $\mathsf{zd}(M) := \{\, a \in R \mid \exists\, x \in M : x \neq 0 \text{ and } ax = 0 \,\}$ and suppose $R \neq 0$ is non-zero, noetherian ring. Then $\mathsf{zd}(M)$ also is the union of all its associated prime ideals. Formally that is

$$\bigcup \mathsf{Sann}(M) \;=\; \mathsf{zd}(M) \;=\; \bigcup \mathsf{Anns}(M)$$

(viii) Let $\mathcal{S} \subseteq \mathsf{Sann}(M)$ be an arbitrary subset of the annihilator spectrum of M, then there is a sub-module $P \leq_{\mathsf{m}} M$ of M satisfying the properties

$$\begin{aligned} \mathsf{Sann}(P) &= \mathcal{S} \\ \mathsf{Sann}\left(M \Big/ P\right) \cap \mathsf{Sann}(P) &= \emptyset \\ \mathsf{Sann}(M) \setminus S &\subseteq \mathsf{Sann}\left(M \Big/ P\right) \end{aligned}$$

(5.9) Example:
If $(R, +, \cdot)$ is an integral domain and we consider R as an R-module, then for any $a \in R$ with $a \neq 0$ we have $\mathsf{ann}(a) = 0$ and thereby 0 is the only element of the annihliator spectrum

$$\mathsf{Sann}(R) \;=\; \{0\}$$

If R is any commutative ring and $p \in R$ is prime let us consider R/pR as an R-module. Then $a \in \operatorname{ann}(b + pR)$ is equivalent to $ab \in pR$. But as p is prime and $b \notin pR$ this means $a \in pR$. Hence for any $b + pR \neq 0 + pR$ we get

$$\begin{aligned} \operatorname{ann}(b + pR) &= pR \\ \operatorname{Sann}\left(R \Big/ pR\right) &= \{\, pR \,\} \end{aligned}$$

This example illustrates that the quotient module M/P may have annihilators that the base module M did not. In other words the inclusions in (i) above may be strict and need not be equalities

$$\operatorname{Sann}(R) \;=\; \{0\} \;\subset\; \{\, 0,\, pR \,\} \;=\; \operatorname{Sann}(pR) \cup \operatorname{Sann}\left(R \Big/ pR\right)$$

(5.10) Example:
Proposition (5.8.(vi)) is surprisingly strong and widely used. Alas it is untrue in the non-noetherian case and in fact this is the main reason, why the later theorems require the noetherian property. As a counter-example regard the polynomial ring in infinitely many variables $R := \mathbb{Z}[t_1, t_2, t_3, \dots]$ and pick up the following ideal in R

$$\mathfrak{a} \;:=\; \langle t_1^2,\, t_2^2,\, t_3^2,\, \dots \rangle_{\mathrm{i}}$$

That is $\mathfrak{a}$ is generated by the squares t_i^2 of the variables t_i. Then we will see, that the R-module $M := R/\mathfrak{a}$ does not have a single associated prime ideal and thereby

$$\operatorname{Sann}_R\left(R \Big/ \mathfrak{a}\right) \;=\; \emptyset$$

Prob consider any $x = f + \mathfrak{a} \in M$ with $x \neq 0$. We will prove that $\operatorname{ann}(x)$ is *not* prime: By definition $\operatorname{ann}(x) = \{\, g \in R \mid gx = 0 \,\} = \{\, g \in R \mid gf \in \mathfrak{a} \,\}$. Because of $x \neq 0$ we have $f \notin \mathfrak{a}$. As $f \in R$ only has finitely many summands there is some $n \in \mathbb{N}$ such that $f \in \mathbb{Z}[t_1, \dots, t_n]$. As $t_{n+1}^2 \in \mathfrak{a}$ we have $t_{n+1}^2 f \in \mathfrak{a}$ but neither t_{n+1} nor f are elements of $\mathfrak{a}$. Hence $\operatorname{ann}(x)$ is not a prime ideal and as $x \neq 0$ has been arbitrary this means $R/\mathfrak{a}$ does not have a single associated prime ideal.

(5.11) Example: (viz. 1162)

(i) Let $(R, +, \cdot)$ be a PID and M be a non-zero finitely generated R-module, such that $M = M(p)$ for some prime $p \in R$. Then pR is the one and only associated prime ideal of M, that is

$$\operatorname{Sann}(M) \;=\; \{\, pR \,\}$$

(ii) If $(R, +, \cdot)$ is a PID and $a \in R$ with $a \neq 0$, then the associated prime ideals of R/aR are precisely those pR where $p \in R$ is a prime divisor of a. Formally that is

$$\operatorname{Sann}_R\left(R \Big/ aR\right) \;=\; \{\, pR \mid p \in R \text{ prime}, \, p \mid a \,\}$$

(5.12) Proposition: (viz. 1159)
Let $(R,+,\cdot)$ be a commutative ring, $U \subseteq R$ be a multiplicatively closed set and M be an R-module. We regard $U^{-1}M$ as an $U^{-1}R$-module and thereby obtain the following properties:

(i) If $\mathfrak{p} = \mathrm{ann}(x) \in \mathrm{Sann}(M)$ is a prime annihilator (of some $0 \neq x \in M$) such that $\mathfrak{p} \cap U = \emptyset$, then the annihilator of $x/1 \in U^{-1}M$ also is a prime ideal, namely we get

$$U^{-1}\mathrm{ann}(x) \;=\; \mathrm{ann}\left(\frac{x}{1}\right) \;\in\; \mathrm{Sann}_{U^{-1}R}\big(U^{-1}M\big)$$

(ii) Thereby $\mathfrak{p} \mapsto U^{-1}\mathfrak{p}$ is an injective map from the annihilator spectrum of M into the annihilator spectrum of $U^{-1}M$. And if R is a noetherian ring, then this map even is bijective, that is

$$\{\,\mathfrak{p} \in \mathrm{Sann}_R(M) \mid \mathfrak{p} \cap U = \emptyset\,\} \;\longleftrightarrow\; \mathrm{Sann}_{U^{-1}R}\big(U^{-1}M\big) \;:\; \mathfrak{p} \mapsto U^{-1}\mathfrak{p}$$

(iii) The surjectivity in (ii) is due to: If $\mathfrak{p} \in \mathrm{Spec}(R)$ is a finitely generated prime ideal of R, such that $\mathfrak{p} \cap U = \emptyset$ and $U^{-1}\mathfrak{p} \in \mathrm{Sann}(U^{-1}M)$, then $\mathfrak{p} \in \mathrm{Sann}(M)$ is the annihilator of some element of M.

(iv) Let R be a noetherian ring and $\mathcal{S}$ be the subset of all prime annihilator ideals of M, that do not meet U. That is $\mathcal{S} := \{\,\mathfrak{p} \in \mathrm{Sann}(M) \mid \mathfrak{p} \cap U = \emptyset\,\}$. Then there is precisely one sub-module $P \leq_{\mathfrak{m}} M$ of M that satisfies $\mathrm{Sann}(P) = \mathrm{Sann}(M) \setminus \mathcal{S}$ and $\mathrm{Sann}(P) \cap \mathrm{Sann}(M/P) = \emptyset$ and this is the kernel of the canonical homomorphism from M to $U^{-1}M$

$$P \;=\; \mathrm{kn}\left(M \to U^{-1}M \;:\; x \mapsto \frac{x}{1}\right)$$

(5.13) Corollary: (viz. 1161)
Let $(R,+,\cdot)$ be a non-zero, noetherian ring and M be any R-module. If $\mathfrak{p} \in \mathrm{Supp}(M)$ is any ideal in the support of M, then there is an associated prime ideal $\mathfrak{a} \in \mathrm{Sann}(M)$ such that $\mathfrak{a} \subseteq \mathfrak{p}$. From this property we see, that $\mathrm{Sann}(M)$ is contained in $\mathrm{Supp}(M)$ and that the minimal elements of these sets coincide. In particular the intersections of all associated prime ideals resp. of all prime ideals in the support of M yield the same result. Altogether this is

$$\begin{aligned} \mathrm{Sann}(M) &\subseteq \mathrm{Supp}(M) \\ \bigcap \mathrm{Sann}(M) &= \bigcap \mathrm{Supp}(M) \\ \big(\mathrm{Sann}(M)\big)_* &= \big(\mathrm{Supp}(M)\big)_* \end{aligned}$$

(5.14) Theorem: (viz. 1163) **Noetherian Filtration:**
Let $(R,+,\cdot)$ be a non-zero, noetherian ring and M be a finitely generated R-module. Then there are finitely many sub-modules $M_i \leq_{\mathfrak{m}} M$ (where $i \in 0 \ldots n$) and prime ideals $\mathfrak{p}_i \in \mathrm{Spec}(R)$ (where $i \in 1 \ldots n$) such that the M_i and $\mathfrak{p}_i$ combine to yield the follwoing two properties

(1) $0 = M_0 \subset M_1 \subset \ldots \subset M_n = M$

(2) for any $i \in 1 \ldots n$ we have an isomophy of the form $M_i \big/ M_{i-1} \cong_{\mathfrak{m}} R \big/ \mathfrak{p}_i$

Thereby $n \geq \operatorname{rank}(M)$ and the annihilator spectrum of M is contained in the set of ideals of $\mathfrak{p}_1$ to $\mathfrak{p}_n$ which in turn is contained in the support of M. In particular $\operatorname{Sann}(M)$ is finite and we have the inclusions

$$\operatorname{Sann}(M) \quad \subseteq \quad \{\, \mathfrak{p}_1, \ldots, \mathfrak{p}_n \,\} \quad \subseteq \quad \operatorname{Supp}(M)$$

(5.15) Remark:
Let us regard $M = \mathbb{Z}$ as an $R = \mathbb{Z}$-module, for example. We have $\operatorname{Sann}(\mathbb{Z}) = \{0\}$, as $\mathbb{Z}$ is an integral domain and $\operatorname{Supp}(\mathbb{Z}) = \operatorname{Spec}(\mathbb{Z})$ is a given, by (5.6.(iv)). Obviously $0 \subset \mathbb{Z}$ is a noetherian filtration using $\mathfrak{p}_1 = 0$. But we also find a different noetherian filtration $0 \subset 5\mathbb{Z} \subset \mathbb{Z}$. Here we have $\mathfrak{p}_2 = 5\mathbb{Z}$ and $\mathfrak{p}_1 = 0 \trianglelefteq_{\mathfrak{i}} \mathbb{Z}$, which is legit, as $5\mathbb{Z}/0 \cong_{\mathfrak{m}} \mathbb{Z}/0$ are isomorphic, as modules. From this example we can glean a few limitations of this method

- The inclusions $\operatorname{Sann}(M) \subset \{\, \mathfrak{p}_1, \ldots, \mathfrak{p}_n \,\} \subset \operatorname{Supp}(M)$ may both be strict.
- The length n of the filtration is *not* uniquely determined and may well exceed the rank of M, as an R-module. However we also see $\operatorname{rank}(M) \leq \#\operatorname{Supp}(M)$.
- The support $\operatorname{Supp}(M)$ may contain infinitely many elements, even for rank 1 modules over a PID.

(5.16) Corollary: (viz. 1164)
Let $(R, +, \cdot)$ be a non-zero noetherian ring, $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$ be an ideal in R and M be a non-zero, finitely generated R-module. Then we obtain the following three sets of equivalences

(i) For any $x \in M$ let us denote $\mathfrak{a}x := \{\, ax \mid a \in \mathfrak{a} \,\}$, then the following four statements are equivalent

 (a) $\mathfrak{a} \subseteq \operatorname{zd}(M)$
 (b) $\exists\, \mathfrak{p} \in \operatorname{Sann}(M) \,:\, \mathfrak{a} \subseteq \mathfrak{p}$
 (c) $\exists\, x \in M \,:\, x \neq 0$ and $\mathfrak{a}x = \{0\}$
 (d) $\forall\, a \in \mathfrak{a}\ \exists\, x \in M \,:\, x \neq 0$ and $ax = 0$

(ii) The following three statements are equivalent, as well

 (a) $\mathfrak{a} \subseteq \bigcap \operatorname{Sann}(M)$
 (b) $\operatorname{Sann}(M) \subseteq \mathbb{V}(\mathfrak{a})$
 (c) $\exists\, n \in \mathbb{N} \,:\, \mathfrak{a}^n M = 0$

(iii) For any $a \in R$ let us denote the *homothety* $\lambda_a : M \to M : x \mapsto ax$. To say that λ_a is *nilpotent* means $\lambda_a^n = 0 \in \operatorname{end}(M)$ for some $n \in \mathbb{N}$. If now $\mathfrak{p} \trianglelefteq_{\mathfrak{i}} R$ is a prime ideal of R, then the following five statements are equivalent

 (a) $\operatorname{Sann}(M) = \{\, \mathfrak{p} \,\}$
 (b) $\forall\, x \in M$ we have: $x \neq 0 \implies \sqrt{\operatorname{ann}(x)} = \mathfrak{p}$
 (c) $\forall\, a \in R$ we have: λ_a is injective or nilpotent
 (d) $\forall\, a \in R$ we have: $a \in \operatorname{zd}(M) \iff \exists\, n \in \mathbb{N} \,:\, a^n M = 0$
 (e) $\forall\, a \in R$ we have: $a \in \operatorname{zd}(M) \iff \forall\, x \in M\ \exists\, n \in \mathbb{N} \,:\, a^n x = 0$

Nota that in this case we find $\mathfrak{p} = \{ a \in R \mid \lambda_a \text{ is nilpotent} \} = \{ a \in R \mid \exists n \in \mathbb{N} : a^n M = 0 \}$. And this set always is an ideal of R, but not necessarily prime, in general.

(5.17) Definition:
Let $(R, +, \cdot)$ be a commutative ring, $\mathfrak{p} \in \operatorname{Spec}(R)$ be a prime ideal of R and M be an R-module. Then we say that M is **$\mathfrak{p}$-primary**, iff $\mathfrak{p}$ is the one and only associated prime of M, formally iff

$$\operatorname{Sann}(M) \;=\; \{ \mathfrak{p} \}$$

And if $P \leq_{\mathfrak{m}} M$ is a sub-module of M then P is said to be **$\mathfrak{p}$-coprimary in** M iff the quotient module M/P is $\mathfrak{p}$-primary, that is iff $\mathfrak{p}$ is the one and only associated prime ideal of M/P

$$\operatorname{Sann}\left(M \Big/ P \right) \;=\; \{ \mathfrak{p} \}$$

Finally M is said to be **primary**, iff M is $\mathfrak{p}$-primary for some prime ideal $\mathfrak{p} \in \operatorname{Spec}(M)$. Likewise P is said to be **coprimary in** M, if L is coprimary in M for some prime ideal $\mathfrak{p} \in \operatorname{Spec}(M)$.

Nota if R is non-zero, noetherian and M is non-zero, finitely generated, then corollary (5.16.(iii)) boasts a rather extensive list of equivalences to M being a $\mathfrak{p}$-primary module.

(5.18) Example: (viz. 1166)
Let $(R, +, \cdot)$ be a non-zero, noetherian ring and $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$ be an ideal of R, with $\mathfrak{a} \neq R$. Denote $\mathfrak{p} := \sqrt{\mathfrak{a}}$ then $\mathfrak{a}$ is primary, as an ideal of R if and only if $\mathfrak{a}$ is $\mathfrak{p}$-coprimary in R, as an R-module. Explicitly this is

$$\mathfrak{a} \text{ is a primary ideal} \quad\Longleftrightarrow\quad \operatorname{Sann}_R\left(R \Big/ \mathfrak{a} \right) \;=\; \{ \mathfrak{p} \}$$

(5.19) Remark:
This example is the reason why most textbooks (including Bourbaki) say that $P \leq_{\mathfrak{m}} M$ is $\mathfrak{p}$-primary, iff P is $\mathfrak{p}$-coprimary (in our sense). This is a problematic notion however, as it depends not only on P, but also on the parent module M. For this reason we follow the same lines, the CRing project does, hoping to further a modernization of mathematical nomenclature. Also we would like to thank the authors of the CRing project [https://math.uchicago.edu/∼amathew/cr.html] for sharing their insights. In classical literature what we call $\mathfrak{p}$-primary remains undefined or is called $\mathfrak{p}$-coprimary. Effectively the notions of primary and coprimary are interchanged in these textbooks.

(5.20) Proposition: (viz. 1166)
Let $(R, +, \cdot)$ be a commutative ring, $\mathfrak{p} \trianglelefteq_{\mathfrak{i}} R$ be a prime ideal and M be an R-module. Also let P and $P_1, \ldots, P_n \leq_{\mathfrak{m}} M$ be sub-modules of M, then the following statements are true:

(i) If R is non-zero and noetherian, M is finitely generated and $P \neq 0$ is non-zero, then we get the implication: If M is $\mathfrak{p}$-primary, then P is $\mathfrak{p}$-primary, too.

(ii) If for any $k \in 1 \ldots n$ the sub-module P_k is $\mathfrak{p}$-primary (all to the same prime ideal $\mathfrak{p}$), then the sum $P_1 + \cdots + P_n \leq_{\mathfrak{m}} M$ of these sub-modules is $\mathfrak{p}$-primary, too.

(iii) If R is non-zero and noetherian, M is finitely generated and for any $k \in 1 \dots n$ the sub-module P_k of M is $\mathfrak{p}$-coprimary in M (all to the same prime ideal $\mathfrak{p}$), then the intersection $P_1 \cap \dots \cap P_n \leq_{\mathfrak{m}} M$ of these sub-modules is $\mathfrak{p}$-coprimary in M, too.

(iv) Consider a short exact chain $0 \to L \to M \to N \to 0$ of R-modules, then we get the following implication: If both L and N are $\mathfrak{p}$-primary, then M is $\mathfrak{p}$-primary, too.

(5.21) Definition:
Let $(R, +, \cdot)$ be a commutative ring and M be an R-module. Also let $P, Q \leq_{\mathfrak{m}} M$ be any two sub-modules of M, then we define the following notions:

(i) A sub-module $L \leq_{\mathfrak{m}} M$ is said to be **prime** iff any non-zero sub-module P of L has precisely the same annihilators, formally that is the following implication for any sub-module $P \leq_{\mathfrak{m}} L$:

$$P \neq 0 \implies \operatorname{ann}(P) = \operatorname{ann}(L)$$

(ii) A sub-module $P \leq_{\mathfrak{m}} M$ is said to be **irreducible**, iff it is not the intersection of two sub-modules strictly containing P. Formally that is iff for all sub-modules $U, V \leq_{\mathfrak{m}} M$ we get

$$P = U \cap V \implies P = U \text{ or } P = V$$

(5.22) Theorem: (viz. 1167)

(i) If $(R, +, \cdot)$ is a non-zero, noetherian ring, M is a finitely generated R-module and $P \leq_{\mathfrak{m}} M$ is a proper, irreducible sub-module of M then P already is coprimary in M. More explicitly, that is

$$P \neq M,\ P \text{ irreducible} \implies \exists\, \mathfrak{p} \in \operatorname{Spec}(R) : \operatorname{Sann}\left(M \Big/ P\right) = \{\mathfrak{p}\}$$

(ii) Let $(R, +, \cdot)$ be a commutative ring, M be a noetherian R-module and $L \leq_{\mathfrak{m}} M$ be a sub-module of M. Then L admits an **irreducible decomposition**, i.e. there are finitely many sub-modules $P_1, \dots, P_s \leq_{\mathfrak{m}} M$ satisfying the following two properties

(1) $L = P_1 \cap \dots \cap P_s$

(2) P_j is irreducible, for any $j \in 1 \dots s$

(iii) Let $(R, +, \cdot)$ be a non-zero, noetherian ring, M be a finitely generated R-module and $L \leq_{\mathfrak{m}} M$ be any sub-module of M. Then L admits a **reduced primary decomposition**, that is there is some $1 \leq s \in \mathbb{N}$ and for any $i \in 1 \dots s$ there are a sub-module $P_i \leq_{\mathfrak{m}} M$ and a prime ideal $\mathfrak{p}_i \in \operatorname{Spec}(R)$, such that the following four properties hold true:

(1) $L = P_1 \cap \dots \cap P_s$

(2) $\forall\, i \in 1 \dots s$ we get $L \neq \bigcap_{j \neq i} P_j$

(3) $\forall\, i \in 1 \dots s$ we get P_i is $\mathfrak{p}_i$-coprimary in M

(4) $\forall\, i, j \in 1 \dots s$ we get $\mathfrak{p}_i = \mathfrak{p}_j \implies i = j$

Nota hereby properties (1) and (3) constitute a *primary decomposition* of L. And in presence of (2) and (4) we speak of a *reduced* decomposition.

(iv) We continue with (iii): If $U \subseteq R$ is a multiplicatively closed set, then we regard $U^{-1}L$ and $U^{-1}P_i$ as $U^{-1}R$-sub-modules of $U^{-1}M$. And thereby $\{ U^{-1}P_i \mid i \in 1 \dots s, \mathfrak{p}_i \cap U = \emptyset \}$ is a reduced primary decomposition of $U^{-1}L$ where $U^{-1}P_i$ belongs to the prime ideal $U^{-1}\mathfrak{p}_i \in \operatorname{Spec}(U^{-1}R)$.

Nota this decomposition has some further useful properties: For any $i \in 1 \dots s$ with $\mathfrak{p}_i \cap U \neq \emptyset$ we even find $U^{-1}P_i = U^{-1}M$ and if $\mathfrak{p}_i \cap U = \emptyset$ we get $P_i = \kappa^{-1}(U^{-1}P_i)$, which explicitly reads as

$$P_i \;=\; \{ x \in M \mid \exists\, u \in U \,:\, ux \in P_i \}$$

(5.23) Corollary: (viz. 1170) **Primary Decomposition:**
Let $(R, +, \cdot)$ be a non-zero, noetherian ring, M be a finitely generated R-module and $L \leq_{\mathfrak{m}} M$ be any sub-module of M. Also let $P_1, \dots, P_s$ be a reduced primary decomposition of L and for $i \in 1 \dots s$ denote the prime ideal associated to M/P_i by $\mathfrak{p}_i$. This is (5.22.(iii)). Then we find further properties:

(i) The following map is an injective homomorphism of R-modules. Thereby, as any P_i is $\mathfrak{p}_i$-coprimary, we have $\operatorname{Sann}(M/P_i) = \mathfrak{p}_i$ for any $i \in 1 \dots n$

$$M \big/ L \hookrightarrow \bigoplus_{i=1}^{s} M \big/ P_i \;:\; x + L \mapsto (x + P_i)$$

(ii) The prime ideals $\mathfrak{p}_i$ are precisely the associated primes M/L. In particular the set $\{ \mathfrak{p}_1, \dots, \mathfrak{p}_s \}$ of the prime ideals occuring in the decomposition is uniquely determined

$$\operatorname{Sann}\left(M \big/ L \right) \;=\; \{ \mathfrak{p}_1, \dots, \mathfrak{p}_s \}$$

(iii) If $\mathfrak{p}_k$ is a minimal element of $\{ \mathfrak{p}_1, \dots, \mathfrak{p}_s \}$ [i.e. there is no $i \in 1 \dots s$ such that $\mathfrak{p}_i \subset \mathfrak{p}_k$] then P_k is uniquely determined, as it is given to be the following sub-module of M

$$P_k \;=\; \{ x \in M \mid \exists\, u \in R \setminus \mathfrak{p}_k \,:\, ux \in L \}$$

$$P_k \big/ L \;=\; \operatorname{kn}\left(M \big/ L \to \left(M \big/ L \right)_{\mathfrak{p}_k} \;:\; x + L \mapsto \frac{x + L}{1} \right)$$

(5.24) Example:

(i) Consider $R = \mathbb{Z}$ and $M = \mathbb{Z} \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_{25}$, then M has the following associated prime ideals $\mathfrak{p}_k$ and corresponding $\mathfrak{p}_k$-coprimary ideals in M, given in the table below

k	$\mathfrak{p}_k = \operatorname{ann}(x)$	x	P_k
0	0	$(1, 0 + 7\mathbb{Z}, 0 + 25\mathbb{Z})$	$0 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_{25}$
1	$7\mathbb{Z}$	$(0, 1 + 7\mathbb{Z}, 0 + 25\mathbb{Z})$	$\mathbb{Z} \oplus 0 \oplus \mathbb{Z}_{25}$
2	$5\mathbb{Z}$	$(0, 0 + 7\mathbb{Z}, 5 + 25\mathbb{Z})$	$\mathbb{Z} \oplus \mathbb{Z}_7 \oplus 0$

Clearly $M = P_0 \cap P_1 \cap P_2 = 0$ is a reduced primary decomposition of the zero-module $L = 0$ is M. Note that $\{ \mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_2 \}$ is uniquely determined by $\mathrm{Sann}(M)$. Also, as $\mathfrak{p}_0 = 0$ is minimal, $\mathcal{P}_0$ also is uniquely determined, in fact $P_0 = \mathrm{tor}(M)$. Yet P_1 and P_2 are *not* uniquely determined, e.g. we could replace P_2 by P_2' where we let

$$P_2' \ := \ \{ (k, k + 7\mathbb{Z}, 0 + 25\mathbb{Z}) \mid k \in \mathbb{Z} \}$$

(ii) Again for $R = \mathbb{Z}$ we take a look, at $M = \mathbb{Z}^2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{25}$. Then M has two associated primes $\mathfrak{p}_0$ and $\mathfrak{p}_1$, only. As above, the following table also gives the corresponding $\mathfrak{p}_k$-coprimary ideals in M

k	$\mathfrak{p}_k = \mathrm{ann}(x)$	x	P_k
0	0	$(1, 0, 0 + 5\mathbb{Z}, 0 + 25\mathbb{Z})$	$0^2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{25}$
1	$5\mathbb{Z}$	$(0, 0, 0 + 5\mathbb{Z}, 5 + 25\mathbb{Z})$	$\mathbb{Z}^2 \oplus 0 \oplus 0$

Then $M/P_0 \ \cong_{\mathsf{m}} \ \mathbb{Z}^2$ which is torsion-free such that $\mathfrak{p}_0 = 0$ is the one and only associated prime of M/P_0. And $M/P_1 \ \cong_{\mathsf{m}} \ \mathbb{Z}_5 \oplus \mathbb{Z}_{25}$, which is annihilated by $5 \in \mathbb{Z}$ such that M/P_1 is $\mathfrak{p}_1$-coprimary in M where $\mathfrak{p}_1 = 5\mathbb{Z}$. We hence see, that the number s of coprimary components occuring in the decomposition be fewer than the rank of M.

(5.25) Example:
Generally if $(M, +, \cdot)$ is a PID, $s \in \mathbb{N}$ and for any $j \in 1 \ldots s$ let $p(j) \in R$ be a prime element of R, such that the $p(j)$ are non-associated, that is for any $j, k \in 1 \ldots s$ we suppose $p(j) \approx q(k) \implies j = k$. Also for any $j \in 1 \ldots s$ let $1 \leq I(j) \in \mathbb{N}$ and for $i \in 1 \ldots I(j)$ let $1 \geq n(i, j) \in \mathbb{N}$. Then we regard the R-module [the torsion part of *any* finitely generated R-module can be written in this form, by (5.32.(v))]

$$M \ := \ \bigoplus_{j=1}^{s} \bigoplus_{i=1}^{I(j)} R \Big/ p(j)^{n(i,j)} R$$

We have already seen in (5.4) that for any $k \in 1 \ldots s$ the p_k-primary component of M is given to be the following [we have also seen $M(q) = 0$ for any $q \in R$ prime, that is *not* associated to any of the p_k]

$$M(p_k) \ = \ \bigoplus_{i=1}^{I(k)} R \Big/ p(k)^{n(i,k)} R$$

In particular we find that $M = M(p_1) \oplus \cdots \oplus M(p_k)$ is the inner direct sum of $p_k R$-primary components, as we have seen $\mathrm{Sann}(M(p_k)) = \{ p_k R \}$ in (5.11.(i)). For any $k \in 1 \ldots s$ let us now denote

$$P_k \ := \ \widehat{M}_k \ = \ \bigoplus_{j \neq k} M(p_j)$$

Then $M/P_k \ \cong_{\mathsf{m}} \ M(p_k)$ and from this it is clear that we have found a reduced primary decomposition of the zero-sub-module $L = 0$ in M

$$P_1 \cap \cdots \cap P_s \ = \ 0$$

In particular (5.23) tells us that we have an embedding of the following form, [but as $M/P_k \cong_{\mathfrak{m}} M(p_k)$ again and $M = M(p_1) \oplus \cdots \oplus M(p_k)$ this even is an isomorphism in this case]

$$M = {}^{M}\big/_{L} \hookrightarrow \bigoplus_{j=1}^{s} {}^{M}\big/_{P_j} : x \mapsto (x + P_j)$$

As all the p_kR are minimal in $\{ p_jR \mid j \in 1 \ldots s \}$ here, the p_kR-coprimary components of M are uniquely determined. This becomes untrue, as soon, as we also gain 0 as an associated primary ideal of M, by adding a non-torsion part $N := \mathbb{Z}^f \oplus M$ to M. In this case

$$\mathrm{Sann}(N) = \{ 0, p_1R, \ldots, p_sR \}$$

so for convenience let $p_0 := 0 \in R$. We also have to modify all the P_k before, by adding $Q_k := \mathbb{Z}^f \oplus P_k$. If we also let $Q_0 := 0 \oplus M$, then Q_k is p_kR-coprimary in N, as $N/Q_0 \cong_{\mathfrak{m}} \mathbb{Z}^f$ and for any $k \in 1 \ldots s$ we still have $N/Q_k \cong_{\mathfrak{m}} M(p_k)$. Thus we have gained a reduced irreducible decomposition of 0 again

$$(0 \oplus M) \oplus \bigoplus_{j=1}^{s} {}^{\mathbb{Z}^f \oplus M}\big/_{\mathbb{Z}^f \oplus P_j} = 0 \leq_{\mathfrak{m}} \mathbb{Z}^f \oplus M$$

5.2 Invariant Factors

In this section we will present a complete classification of finitely generated modules over PIDs. Note that this encompasses finitely generated abelian groups, as these can be regarded as $\mathbb{Z}$-modules under the scalar multiplication $\mathbb{Z} \times G \to G : (k, g) \mapsto g^k$. So let us outline the ultimate goal of this section: First of all any finitely generated module M over a PID R can be decomposed into

$$M \quad \cong_{\mathsf{m}} \quad M \Big/ \mathsf{TOR}(M) \oplus \mathsf{TOR}(M)$$

This is due to the fact that $M/\mathsf{TOR}(M)$ is torsion-free and finitely generated and over a PID this implies that $M/\mathsf{TOR}(M)$ even is free. So the torsion-free part $M/\mathsf{TOR}(M)$ of M is free and hence of the form R^f for some $f \in \mathbb{N}$. It remains to study the torsion-part $\mathsf{TOR}(M)$. It will turn out, that this part is of the form

$$\mathsf{TOR}(M) \quad \cong_{\mathsf{m}} \quad \bigoplus_{i=1}^{r} R \Big/ d_i R$$

This is not so much of a surprise, as $R/\mathrm{ann}(x) \xrightarrow{\sim} Rx$ is true for any $x \in M$ and $\mathsf{TOR}(M)$ is finitely generated again. But if we do it right, we can arrange the *invariant factors* d_i in such a way, that they form an ascending chain under the division relation $d_1 \mid d_2$, $d_2 \mid d_3$ and so on until $d_{n-1} \mid d_n$. And it turns out that these d_i are unique up to associatedness.
We will also present two variations of this representation of M: By primary decomposition of the invariant factors and application of the Chinese remainder theorem, we also find a form using *elementary divisors*: That is there are (distinct) primes $p(j) \in R$ and powers $1 \leq n(i,j) \in \mathbb{N}$ such that the torsion-part is of the form

$$\mathsf{TOR}(M) \quad \cong_{\mathsf{m}} \quad \bigoplus_{j=1}^{s} \bigoplus_{i=1}^{I(j)} R \Big/ p(i)^{n(i,j)} R$$

It is this form from which we can also construct the primary decomposition of M, as we have already outlined in section 5.1, refer to (5.25) for details. But of course these external isomorphies define the inner structure of M. If M is a non-zero, finitely generated module over a PID, it can be written as an inner direct sum of cyclic sub-modules

$$M \quad = \quad \bigoplus_{i=1}^{n} Rm_i$$

such that $\mathrm{ann}(m_1) \supseteq \ldots \supseteq \mathrm{ann}(m_n)$. Thereby the chain of annihilators has the length $n = \mathrm{rank}(M)$ and is uniquely determined. This is another consequence of the invariant factor form. We will present a remark that describes in detail how to get from one form to the other.
Later on the chain of invariant ideals will play an important role in canonical form theory: If V is a finitely generated vector space over a field F and $\varphi : V \to V$ is linear, then V can be turned into an $F[t]$-module. But as $F[t]$ is a PID, we can decompose V into cyclic sub-modules and thereby study φ. But in order to get to that point we need some more tools, most notably the notion of a *primitive* element $p \in M$ and the *content* of an element $x \in M$.

(5.26) Definition: (viz. 1171)

(i) Let $(R,+,\cdot)$ be a commutative ring and M be an R-module. Then an element $p \in M$ is said to be **primitive** iff for any $x \in M$ and any $a \in R$ we get the implication

$$p = ax \implies a \in R^*$$

(ii) If $(R,+,\cdot)$ be a commutative ring, M is an R-module and $P \leq_{\mathsf{m}} M$ is a sub-module of M, then we recall the definition of the **hull** of P to be the set of all $x \in M$ that have a multiple in P, that is

$$\mathrm{Hull}(P) := \{\, x \in M \mid \exists\, a \in R : a \neq 0 \text{ and } ax \in P \,\}$$

If R is an integral domain, then $\mathrm{Hull}(P)$ is a sub-module of M that contains P and all torsion elements of M, i.e. we have $P + \mathrm{tor}(M) \subseteq \mathrm{Hull}(P) \leq_{\mathsf{m}} M$.

(iii) If $(R,+,\cdot)$ is an UFD and $M \neq 0$ is a non-zero free R-module with basis $\{\, m_i \mid i \in I \,\}$ then for any $x \in M$ we define the **content** of x to be the greatest common divisor of the coefficients of x

$$\mathrm{cont}(x) := \gcd\{\, a_i \mid i \in I \,\} \quad \text{where} \quad x = \sum_{i \in I} a_i m_i$$

Recall that thereby $c \in \mathrm{cont}(x)$ is equivalent, to $\mathrm{cont}(x) = cR^*$, as the greatest common divisor is is unique up to associatedness. And note that this is well defined, that is independent of the choice of the basis of M. If $\{\, n_i \mid i \in I \,\}$ is another basis of M and $x = \sum_i b_i n_i$ then we have $\gcd\{\, a_i \mid i \in I \,\} = \gcd\{\, b_i \mid i \in I \,\}$.

(5.27) Example:

(i) The 3-tuple $x = (4,6,0) \in \mathbb{Z}^3$ is not primitive, as it can be written as $x = 2p$ where $p = (2,3,0) \in \mathbb{Z}^3$. Clearly p is primitive, as we cannot pull out any common factor of the coefficients, as $1 \in \gcd\{\, 2,3,0 \,\}$. This example illustrates that p is primitive if and only if $\mathrm{cont}(p) = 1$, which we will prove next.

(ii) If F is a field and V is an F-vector space, then $p \in V$ is primitive if and only if $p \neq 0$ is non-zero.

Prob $0 \in V$ is not primitive, as $0 = 0x$ for any $x \in V$ and $0 \notin F^*$. Conversely if $p \neq 0$ then $p = ax$ implies $a \neq 0$ and hence $a \in F^*$. Admittedly this is somewhat artifical, but true nevertheless.

(iii) If R is a commutative ring and we regard $M = R$ as an R-module itself, then $p \in M$ is primitive, if and only if $p \in R^*$.

Prob clearly $p = p \cdot 1$ is generally true. But if p is primitive, this implies $p \in R^*$. And conversely if $p \in R^*$, then $p = ax$ yields $1 = (ax)p^{-1} = a(xp^{-1})$ such that $a \in R^*$.

(iv) If we regard $\mathbb{Q}$ as a $\mathbb{Z}$-module, then $\mathbb{Q}$ has no primitive elements at all, as always $u/v = 2(u/2v)$ but $2 \notin \mathbb{Z}^*$ is not a unit.

(5.28) Proposition: (viz. 1172)

(i) If $(R,+,\cdot)$ is a commutative ring, M is a noetherian R-module and $x \in M$ an element with $\mathrm{ann}(x) = 0$, then there is some primitive $p \in M$ and some $a \in R$ such that

$$x \;=\; ap$$

(ii) If $(R,+,\cdot)$ is an UFD and M a free R-module, then any $x \in M$ with $x \neq 0$ is primitive, if and only if $\mathrm{cont}(x) = 1$. Formally we find the equivalence of

$$x \text{ is primitive} \quad\Longleftrightarrow\quad 1 \in \mathrm{cont}(x)$$

In particular if we choose any $c \in \mathrm{cont}(x)$, then there is some primitive $p \in M$ such that $x \neq 0$ can be written in the following form

$$x \;=\; cp$$

(iii) If $(R,+,\cdot)$ is a PID, M is a free R-module and $p \in M$ is any fixed primitive element of M, then there is a basis $\{ m_i \mid i \in I \}$ of M that contains p, i.e. $p \in \{ m_i \mid i \in I \}$.

(iv) If $(R,+,\cdot)$ is a PID, M is free R-module and $P \leq_{\mathrm{m}} M$ is a finitely generated sub-module of M, then there are a basis $\mathcal{M} = \{ m_i \mid i \in I \}$ of M, a finite subset $\{ p_i \mid i \in 1 \ldots n \} \subseteq \mathcal{M}$ and a set of scalars $\{ d_i \mid i \in 1 \ldots n \} \subseteq R \setminus \{0\}$ that satisfy

(1) $\{ d_i p_i \mid i \in 1 \ldots n \}$ is a basis of P

(2) for any $i \in 2 \ldots n$ we have $d_{i-1} \mid d_i$

(5.29) Remark:

- Let us sketch the proof of (5.28.(iv)) how to find the invariant factors d_i. This is done iteratively, by the rank of P: If $P = 0$ then $n = 0$ and hence there are none. If $P \neq 0$, let $M_1 := M$ and $P_1 := P$ and consider the following set of ideals of R

$$\mathcal{A}_1 \;:=\; \{ \mathrm{cont}(x)R \mid x \in P_1,\, x \neq 0 \}$$

Thereby $\mathrm{cont}(x)R$ is the ideal generated by $\mathrm{cont}(x) \subseteq R$, but this is equivalent to $\mathrm{cont}(x)R = cR$ for an arbitrary $c \in \mathrm{cont}(x)$.

- As R is noetherian (even a PID) the set $\mathcal{A}_1$ of ideals has a maximal element $\mathrm{cont}(x_1)R \in \mathcal{A}_1^*$. Let $d_1 := \mathrm{cont}(x_1)$ and $x_1 = d_1 p_1$ for some primitive $p_1 \in M$. Then we find a basis $\mathcal{M}_1$ of M_1 containing p_1. If we let $\mathcal{M}_2 := \mathcal{M}_1 \setminus \{ p_1 \}$, $M_2 := \mathrm{Lh}(\mathcal{M}_2)$ and $P_2 := P_1 \cap M_2$ then

$$P_1 \;=\; Rx_1 \oplus P_2$$

- So we can commence with P_2 in the same way: Define $\mathcal{A}_2$, pick some $x_2 \in P_2$ such that $\mathrm{cont}(x_2)R$ is maximal in $\mathcal{A}_2$, write $x_2 = d_2 p_2$ and so on until $P_{n+1} = 0$. By construction $\{ p_1, \ldots, p_n \} \cup \mathcal{M}_{n+1}$ is a basis of M and $\{ x_1, \ldots, x_n \} = \{ d_1 p_1, \ldots, d_n p_n \}$ is a basis of P. And the respective maximality of $\mathrm{cont}(x_i)R \in \mathcal{A}_i$ ensures $d_{i-1} \mid d_i$.

(5.30) Example:
The following example will illustrate (5.28.(iv)): As the base module we choose $M := \mathbb{Z}^3$. Now let $x_1 := (2,4,0)$, $x_2 := (2,-2,0)$ and $x_3 := (4,20,0)$. Let $P := \mathrm{Lh}\{\, x_1, x_2, x_3 \,\}$ be the sub-module of M generated by x_1 to x_3. In other words P is given to be

$$P \;:=\; \mathrm{im}\begin{pmatrix} 2 & 2 & 4 \\ 4 & -2 & 20 \\ 0 & 0 & 0 \end{pmatrix} \;\leq_{\mathrm{m}}\; \mathbb{Z}^3$$

Clearly $\mathrm{cont}(x_1) = \mathrm{cont}(x_2) = 2$ and $\mathrm{cont}(x_3) = 4$. Thus $2\mathbb{Z}$ is the maximal ideal of $\mathcal{A}_1$ and we take $d_1 := 2$. In general there may be several ideals maximal in $\mathcal{A}_1$. In this case the natural choice is x_1 for an element with maximal content such that $p_1 = (1,2,0)$, as $d_1 p_1 = x_1$. We can append $\{\, p_1 \,\}$ to a basis $\{\, p_1, m_2, m_3 \,\}$ of M by taking $m_2 := (0,1,0)$ and $m_3 := (0,0,1)$. Then $M_2 = 0 \oplus \mathbb{Z}^2$ and

$$P_2 \;=\; P_1 \cap M_2 \;=\; \{\, (0, 4a - 2b + 20c, 0) \mid 2a + 2b + 4c = 0 \,\}$$

where a, b and $c \in \mathbb{Z}$. The condition $2a + 2b + 4c = 0$ can be rewritten as $b = -a - 2c$ and inserting this into P_2 we find the following presentation of P_2

$$P_2 \;=\; \{\, (0, 6(a + 4c), 0) \mid a, c \in \mathbb{Z} \,\} \;=\; 0 \oplus 6\mathbb{Z} \oplus 0$$

That is $d_2 = 6$ and $p_2 = (0,1,0) = m_2$. In this lucky case $\{\, p_2, m_3 \,\}$ is a basis of M_2 again such that $\{\, d_2 p_2 \,\}$ is a basis of P_2. Since $M_3 = 0^2 \oplus \mathbb{Z}$ and $P_3 = P_2 \cap M_3 = 0$ we are done. Altogether we have found a basis $\{\, p_1, p_2, m_3 \,\}$ and $\{\, d_1, d_2 \,\}$ such that $\{\, d_1 p_1, d_2 p_2 \,\}$ is a basis of P. Hereby $d_1 p_1 = (2,4,0) = x_1$ and $d_2 p_2 = (0,6,0)$.

By now we have all the ingredients needed for the proof of the classification of finitely generated modules over PIDs. Note however that the sequel of proves does not match the order in which the theorems are given. To us the invariant factor form seems to be the natural choice, but there are direct approaches to the forms of invariant ideals and elementary divisors, as well.
So let us first study modules that are in invariant factor form - these are well-behaved even over UFDs. After that we will prove that over a PID any finitely generated module is isomorphic to such a module. And the other two forms will be derived from the invariant factor form.

(5.31) Proposition: (viz. 1175)
Let $(R, +, \cdot)$ be an integral domain, f, $r \in \mathbb{N}$ and $\{\, d_1, \ldots, d_r \,\} \subseteq R^\bullet$ be non-zero, non-unit elements of the base ring such that for any $i \in 2 \ldots r$ we have the divisibility condition $d_{i-1} \mid d_i$. Then we get the following statements concerning the R-module

$$M \;:=\; R^f \oplus T \quad \text{where} \quad T \;:=\; \bigoplus_{i=1}^{r} R \Big/ d_i R$$

(i) $\mathrm{free}(M) \;=\; f$

(ii) $\mathrm{ann}(T) \;=\; d_r R$

(iii) $\mathrm{TOR}(M) \;=\; \{0\}^f \oplus T$

(iv) M is free if and only if $r = 0$

(v) M is a torsion-module if and only if $f = 0$

And if R even is an UFD we can also control the rank of this module M, as we find the equalities of

(vi) $\mathrm{rank}(T) \;=\; r$

(vii) $\mathrm{rank}(M) \;=\; f + r$

(5.32) Theorem: (viz. 1177)
Let $(R, +, \cdot)$ be a PID and M a finitely generated module over R. Then we find the following statements:

(i) **Invariant Ideals:** If $M \neq 0$ is non-zero and $n := \mathrm{rank}(M) < \infty$ is finite, then there are some $m_1, \ldots, m_n \in M \setminus \{0\}$ such that M is the inner direct sum

$$M \;=\; Rm_1 \oplus \cdots \oplus Rm_n$$

and $\mathrm{ann}(m_1) \supseteq \mathrm{ann}(m_2) \supseteq \ldots \supseteq \mathrm{ann}(m_n) = \mathrm{ann}(M)$. This descending chain of ideals in R is said to be the chain of *invariant ideals* of M. And in this case for any $i \in 2 \ldots n$ we also get

$$\mathrm{ann}(m_{i-1}) \;=\; \mathrm{ann}\left(M \Big/ Rm_i + \cdots + Rm_n \right)$$

(ii) The chain of invariant ideals of M is uniquely determined, that is: Suppose $m, n \in \mathbb{N}$ and let $p_1, \ldots, p_m$ and $q_1, \ldots, q_n \in M \setminus \{0\}$ be some vectors, such that M is the inner direct sums

$$\bigoplus_{i=1}^{m} Rp_i \;=\; M \;=\; \bigoplus_{j=1}^{n} Rq_j$$

and $\mathrm{ann}(p_1) \supseteq \ldots \supseteq \mathrm{ann}(p_m)$ and $\mathrm{ann}(q_1) \supseteq \ldots \supseteq \mathrm{ann}(q_n)$. Then we already have $m = n$ and for any $i \in 1 \ldots n$ we also get the equality of the annihilator ideals

$$\mathrm{ann}(p_i) \;=\; \mathrm{ann}(q_i)$$

(iii) **Invariant Factors:** If $M \neq 0$ is non-zero and finitely generated, then there are some $f, r \in \mathbb{N}$ and a set $\{ d_i \mid i \in 1 \ldots r \} \subseteq R$ of scalars, such that the following three properties are satisfied

(1) for any $i \in 1 \ldots r$ we have $d_i \in R^\bullet$

(2) for any $i \in 2 \ldots r$ we have $d_{i-1} \mid d_i$

(3) M is isomorphic, as an R-module, to the direct sum:

$$M \;\cong_{\mathfrak{m}}\; \bigoplus_{i=1}^{r} R \Big/ d_i R \oplus R^f$$

A set of scalars $\{ d_i \mid i \in 1 \dots r \} \subseteq R$ that satisfies the properties (1) to (3) above is called *invariant factors* of M. And thereby we get the additional properties

$$\begin{aligned} f &= \mathsf{free}(M) \\ f + r &= \mathsf{rank}(M) \\ r = 0 &\iff M \text{ is free} \\ f = 0 &\iff M \text{ is a torsion-module} \end{aligned}$$

(iv) If $M \neq 0$ is non-zero and finitely generated, then the invariant factors of M are *essentially* unique, in the following sense: If $g \in \mathbb{N}$ and $\{ e_j \mid j \in 1 \dots s \} \subseteq R$ is another set of invariant factors of M

$$\begin{aligned} M &\cong_{\mathsf{m}} \bigoplus_{i=1}^{r} R \Big/ d_i R \oplus R^f \\ M &\cong_{\mathsf{m}} \bigoplus_{j=1}^{s} R \Big/ e_j R \oplus R^g \end{aligned}$$

then we already have $f = g$ and $r = s$ and for any $i \in 1 \dots r$ there is some unit $u_i \in R^*$ such that

$$e_i = u_i d_i$$

(v) **Elementary Divisors:** If $M \neq 0$ is non-zero and finitely generated, then there are some $f, s \in \mathbb{N}$, a set $\{ p(j) \mid j \in 1 \dots s \} \subseteq R$ of prime elements of R and powers $n(i,j) \in \mathbb{N}$ (where $i \in 1 \dots I(j)$), such that for any $j, k \in 1 \dots s$ the following three properties are satisfied

(1) $p(j) \approx p(k) \implies j = k$

(2) $n(1,j) \geq n(2,j) \geq \cdots \geq n(I(j),j) \geq 1$

(3) M is isomorphic, as an R-module, to the following direct sum:

$$M \cong_{\mathsf{m}} \bigoplus_{j=1}^{s} \bigoplus_{i=1}^{I(j)} R \Big/ p(j)^{n(i,j)} R \oplus R^f$$

A set of prime elements $\{ p(j) \mid j \in 1 \dots s \} \subseteq R$ and powers $\{ (n(i,j) \mid j \in 1 \dots s, i \in 1 \dots I(j) \}$ that satisfies the properties (1) to (3) above are called *elementary divisors* of M.

(vi) If $M \neq 0$ is non-zero and finitely generated, then the elementary divisors of M are *essentially* unique, in the following sense: If $g \in \mathbb{N}$ and $\{ e_j \mid j \in 1 \dots s \} \subseteq R$ is another set of elementary divisors of M

$$\begin{aligned} M &\cong_{\mathsf{m}} \bigoplus_{j=1}^{s} \bigoplus_{i=1}^{I(j)} R \Big/ p(j)^{n(i,j)} R \oplus R^f \\ M &\cong_{\mathsf{m}} \bigoplus_{\ell=1}^{t} \bigoplus_{k=1}^{K(\ell)} R \Big/ q(\ell)^{m(k,\ell)} R \oplus R^g \end{aligned}$$

then we already have $f = g$ and $s = t$ and there is a permutation $\sigma : 1 \dots s \longleftrightarrow 1 \dots t$ such that

for any $j \in 1 \ldots s$ and any $i \in 1 \ldots I(j)$

(1) $p(j) \approx q(\sigma(j))$

(2) $I(j) = K(\sigma(j))$

(3) $n(i,j) = m(i,\sigma(j))$

(5.33) Remark:

- Theorem (iii) is an ultimate consequence of proposition (5.28): As M is finitely generated there is some epimorphism $\psi : R^n \twoheadrightarrow M$ where $n = \mathrm{rank}(M)$. Let $P := \mathrm{kn}(\psi)$ be kernel of that epimorphism, which is a sub-module of R^n. Then we can apply (5.28.(iv)) to P such that there is a basis $\{ p_1, \ldots, p_r, m_1, \ldots, m_f \}$ of R^n and $\{ d_1, \ldots, d_r \} \subseteq R$ such that $\{ d_i p_i \mid i \in 1 \ldots r \}$ is a basis of P. Then R^n/P can be written as a direct sum of R/d_iR. As $n = \mathrm{rank}(M)$ there are no $d_i \in R^*$. And any m_j that occurs in the basis of R^n but not among the $\{ p_1, \ldots, p_r \}$ adds an R to this direct sum. Then the first isomorphism theorem $R^n/P \xrightarrow{\sim} M$ can be twisted, as to give the desired isomorphy.

- If the base ring R even is an Euclidean domain (and not only a PID) we can omit the preparations of (5.28), as we can replace theorem (iv) by (4.88.(iii)). Here's how: If $n := \mathrm{rank}(M)$ and we pick up some generators $M = \mathrm{Lh}\{ x_1 \ldots, x_n \}$ then we have an epimorphism

$$\varrho \; : \; R^n \twoheadrightarrow M \; : \; (b_i) \mapsto \sum_{i=1}^{n} b_i x_i$$

Thereby $\mathrm{kn}(\varrho) \leq_{\mathsf{m}} R^n$ is a free module, as R^n is free and R is a PID. That is there is a basis $\{ a_1, \ldots, a_r \} \subseteq R^n$ of $\mathrm{kn}(\varrho)$. If we denote the matrix $A := (a_1\, a_2 \ldots a_r) \in \mathrm{mat}_{n,r}(R)$ with the columns $\mathrm{col}_i(A) = a_i$, then $\mathrm{kn}(\varrho) = \mathrm{Lh}\{ a_1, \ldots, a_r \} = \mathrm{im}(A)$. But we can use (4.88.(iii)) to turn A into the form

$$\begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_r \\ 0 & \ldots & 0 \\ \vdots & & \vdots \\ 0 & \ldots & 0 \end{pmatrix} = D = SAT = S \begin{pmatrix} | & & | \\ a_1 & \cdots & a_r \\ | & & | \end{pmatrix} T$$

where $S \in \mathrm{gl}_n(R)$, $T \in \mathrm{gl}_r(R)$ and $d_{i-1} \mid d_i$ for any $i \in 2 \ldots r$. Thereby the d_i are the invariant factors of M, so we have found an alternative way of computing these (for Euclidean domains). Let us argue, why: As $D = SAT$ we have $A = S^{-1}DT^{-1}$ and thereby $\mathrm{im}(A) = S^{-1}\mathrm{im}(D)$ by (4.45.(iii)). But $\mathrm{im}(D) = d_1R \oplus \cdots \oplus d_rR \oplus 0^f$ (where $f := n - r$) and thereby we have

$$\bigoplus_{i=1}^{r} R \Big/ d_iR \oplus R^f \; = \; R^n \Big/ \mathrm{im}(D) \; \xrightarrow{\sim} \; R^n \Big/ \mathrm{kn}(\varrho)$$

where the isomorphism is given by $b + \mathrm{im}(D) \mapsto S^{-1}b + \mathrm{kn}(\varrho)$. Thus we have found a decomposition of M with the d_i as invariant factors:

$$\bigoplus_{i=1}^{r} R \Big/ d_i R \oplus R^f \quad \xrightarrow{\sim} \quad M \ : \ b + \mathrm{im}(D) \mapsto \varrho\big(S^{-1}b\big)$$

(5.34) Remark:
Let $(R, +, \cdot)$ be a PID and M be a non-zero, finitely generated R-module. Then we find the following correspondences between these forms of M:

- *Invariant Factors to Invariant Ideals:* Consider M in the invariant factor form of (5.32.(iii)), let $n := r + f = \mathrm{rank}(M)$ and $d_j := 0$ for any $j > r$. Then $R/d_jR = R$ and $d_{i-1} \mid d_i$ is true for any $i \in 2 \ldots n$, such that the isomorphism takes the form

 $$\Phi \ : \ \bigoplus_{i=1}^{n} R \Big/ d_i R \quad \xrightarrow{\sim} \quad M$$

 For any $j \in 1 \ldots n$ let $g_j := (\delta_{i,j} + d_i R)$ be the canonical generators of the module on the left side. Then the $m_j := \Phi(g_j) \in M$ generate $M = Rm_1 \oplus \cdots \oplus Rm_n$ of M and $\mathrm{ann}(m_j) = \mathrm{ann}(g_j) = d_i R$ such that we have the chain $\mathrm{ann}(m_1) \ \supseteq \ \ldots \ \supseteq \ \mathrm{ann}(m_n)$ of invariant ideals.

- *Invariant Ideals to Invariant Factors:* If $M = Rm_1 \oplus \cdots \oplus Rm_n$ such that $\mathrm{ann}(m_1) \ \supseteq \ \ldots \ \supseteq \ \mathrm{ann}(m_n)$ then we let $d_i R = \mathrm{ann}(m_i)$ and $r := \max\{\, i \in 1 \ldots n \mid \mathrm{ann}(m_i) \neq 0 \,\}$. If we now regard the epimorphism

 $$\varrho \ : \ R^n \ \twoheadrightarrow \ M \ : \ (a_i) \mapsto \sum_{i=1}^{n} a_i m_i$$

 then $\mathrm{kn}(\varrho) = d_1 R \oplus \cdots \oplus \ldots d_r R \oplus 0^f$ where $f = n - r$. Thereby the d_i are the invariant factors of M and we find the isomorphism

 $$\Phi \ : \ \bigoplus_{i=1}^{r} R \Big/ d_i R \oplus R^f \quad \xrightarrow{\sim} \quad M \ : \ (a_i) + \mathrm{kn}(\varrho) \mapsto \sum_{i=1}^{n} a_i m_i$$

- *Invariant Factors to Elementary Divisors:* If M is in invariant factor form again (as above) and we look at the isomorphy

 $$\Phi \ : \ \bigoplus_{i=1}^{r} R \Big/ d_i R \oplus R^f \quad \xrightarrow{\sim} \quad M$$

 Then we use a decomposition of d_r into prime factors $d_r = \alpha_r p(1)^{n(1)} \ldots p(s)^{n(s)}$ where the $p(j) \in R$ are pairwise non-associated primes and $n(j) \geq 1$. Then, as $d_i \mid d_r$ all the d_i have the a prime decomposition of the form

 $$d_i \quad = \quad \alpha_i \prod_{j=1}^{s} p(j)^{\langle p(j) | d_i \rangle}$$

for any $i \in 1 \dots r$. Let $n(i,j) := \langle p(j) \mid d_{r+1-i} \rangle \in \mathbb{N}$ where $j \in 1 \dots s$ and $i \in 1 \dots r$ and let $I(j) := \#\{ i \in 1 \dots r \mid n(i,j) \neq 0 \}$. Then we found the elementary divisors of M, as

$$\bigoplus_{j=1}^{s} \bigoplus_{i=1}^{I(j)} R \Big/ p(j)^{n(i,j)} R \oplus R^f \quad \xrightarrow{\sim} \quad M$$

In a less formalistic, but easier to understand way, let us build up a table containing the powers of $p(j)$ occuring in the prime factorisation of d_i. Then then powers $n(i,j)$ of the elementary divisors occur in this table, in inverse order

	$p(1)$	$p(2)$	$\cdots$	$p(s)$
d_1	$n(r,1)$	$n(r,2)$	$\cdots$	$n(r,s)$
$\vdots$	$\vdots$	$\vdots$		$\vdots$
d_{r-1}	$n(2,1)$	$n(2,2)$	$\cdots$	$n(2,s)$
d_r	$n(1,1)$	$n(1,2)$	$\cdots$	$n(1,s)$

- *Elementary Divisors to Invariant Factors:* If conversely we have the elementary divisors of M, as in (5.32.(v)): $r := \max\{ I(j) \mid j \in 1 \dots s \}$ and $n(i,j) := 0$ for any $j \in 1 \dots s$ and $I(j) < i \leq r$. Then

$$d_i \quad := \quad \prod_{j=1}^{s} p(j)^{n(r+1-i,j)} \quad \in \quad R$$

are the invariant factors of M (that is: you can use the table above, to multiply up the d_i along the rows of this table) such that we find an isomorphism of the form

$$\bigoplus_{i=1}^{r} R \Big/ d_i R \oplus R^f \quad \xrightarrow{\sim} \quad M$$

5.3 Diagonalization

To begin with let us think of a little geometry: A linear map may dilate (and contract) vectors and even rotate around a certain axis. What a linear map cannot is shift, as $\varphi(0) = 0$ is fixed. E.g. consider

$$A := \begin{pmatrix} 0.5 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \quad B := \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) & 0 \\ \sin(\alpha) & \cos(\alpha) & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{mat}_3(\mathbb{R})$$

Clearly A shrinks any vector $x \in \mathbb{R}^3$ by half in the direction of e_1 (= the x-Axis) and doubles x in the direction of e_3 (= the z-Axis). The direction of e_2 (= the y-Axis) is unaffected. Thus if A is in diagonal form it is plain to see, which direction is dilated by which factor.

B is another interesting example: It rotates any vector $x \in \mathbb{R}^3$ around the e_3-Axis (= z-Axis) by the angle α [if we look down from the positive side of the z-Axis the rotation is counter-clockwise]. Thereby the e_3-coordinate of x remains unchanged. That is any cylinder with $\mathbb{R}e_3$ as its middle axis is invariant under the action of B. Here we see the property the rotation axis must have: It is invariant under the action of φ. That is we look out for vectors $x \in R^n$ such that

$$\varphi(x) \quad = \quad \lambda x$$

for some $\lambda \in R$. These vectors will be called *eigenvectors* of φ [*eigen* is a German word meaning *own* or *self*, so it could be translates as a vector belonging to φ]. The factor λ is the dilation factor of x and will be called *eigenvalue* of φ. It might be appealing to study eigenvectors simply for geometrical reasons, but the theory provides much more: First of all eigenvectors are the fundamental notion of canonical form theory - most notably the Jordan normal form. The Jordan normal form is the key when trying to solve a system of ordinary, linear differential equations (linear ODEs). For example chaos theory relies heavily on this.

In statistics consider the problem: Given data $(x_1, x_2, \ldots, x_n)$ for every single individual within a large group and of course these values x_j vary. There may be certain unknown variables u_i behind the scene, that control entire combinations of the x_j - e.g. a tall person usually has large feet and is heavier. But the colour of eyes is independent of height. An intelligent student will probably have better grades all around, a student who has to work for his living has less time for his studies and may have worse grades. Factor analysis now tries to find the combinations of variables x_j that belong to a common controlling variable u_i. These combinations will be the eigenvectors of the variance matrix of the x_j and the corresponding eigenvalues will be the weights to what extend the variance of this combination contributes to the variance of the entire set of data. In quantum mechanics a linear map φ models an observable such as location, energy or impulse. A vector x models the state the physical system is in - which is a probability distribution over the certain "pure" states. These pure states are the eigenvectors of φ, the eigenvalue λ is the result of measuring φ if the system is in that state.

We could go on with applications of this beautiful theory for quite some time, but by now it should be clear, that it is truly fundamental and closely linked to applications. For now we stick to the case of finitely many dimensions however, which covers most of its applications - but not quantum mechanics. General quantum mechanics requires the theory of unbound operators and also is genuinely stochastic which both is beyond the scope of this textbook.

(5.35) Definition:
Let $(R,+,\cdot)$ be an arbitrary ring, M be an R-module and consider $\varphi \in \mathrm{end}(M)$, that is a linear map $\varphi : M \to M$ from M to itself. Then a sub-module $P \leq_{\mathsf{m}} M$ is said to be **invariant** under φ iff

$$\varphi(P) \quad \subseteq \quad P$$

And a vector $x \in M$ is said to be an **eigenvector** of φ to the **eigenvalue** $\lambda \in R$, if we have the equation

$$\varphi(x) \quad = \quad \lambda\, x$$

The set of all eigenvectors to a given $\lambda \in R$ is called the **eigenspace** of φ to λ. And the set of all eigenvalues of φ is said to be the **spectrum** of φ. We will denote these sets by

$$\begin{array}{rcl} \mathrm{Eig}_\varphi(\lambda) & := & \mathrm{kn}\,(\varphi - \lambda \mathbb{1}_M) \\ & = & \{\, x \in M \mid \varphi(x) = \lambda x \,\} \\ \mathrm{Spec}(\varphi) & := & \Big\{\, \lambda \in R \mid \mathrm{Eig}_\varphi(\lambda) \neq 0 \Big\} \\ & = & \{\, \lambda \in R \mid \exists\, x \in M : x \neq 0 \text{ and } \varphi(x) = \lambda x \,\} \end{array}$$

(5.36) Example: (viz. 960)
Let $(R,+,\cdot)$ is an integral domain, M an R-module and $\varphi \in \mathrm{end}(M)$ be an R-module endomorphism. Suppose there is a basis $\{\, m_1, \ldots, m_n \,\}$ of M, such that for any $j \in 1 \ldots n$ there is some $a_j \in R$ such that $\varphi(m_j) = a_j m_j$ (such an endomorphism will later be called *diagonizable*). Then for any $\lambda \in R$

$$\mathrm{Eig}_\varphi(\lambda) \quad = \quad \mathrm{Lh}\{\, m_j \mid j \in 1 \ldots n,\, a_j = \lambda \,\}$$

In particular all the eigenspaces of a diagonizable endomorphism φ are finitely generated and free R-sub-modules of M again. Their dimension is given to be the number of a_j that equal λ

$$\mathrm{rank}\big(\mathrm{Eig}_\varphi(\lambda)\big) \quad = \quad \#\,\{\, j \in 1 \ldots n \mid a_j = \lambda \,\}$$

(5.37) Proposition: (viz. 960)
Let $(R,+,\cdot)$ be a commutative ring, M be an R-module and $\varphi \in \mathrm{end}(M)$ be a module-endomorphism on M. Then the following statements hold true:

(i) Let $I \neq \emptyset$ be any index set and for any $i \in I$ let $P_i \leq_{\mathsf{m}} M$ be a φ-invariant sub-module of M, then the sum and the intersection of the P_i are φ-invariant sub-modules of M, too

$$\begin{array}{rcl} \varphi\left(\sum\limits_{i\in I} P_i\right) & \subseteq & \sum\limits_{i\in I} P_i \\ \varphi\left(\bigcap\limits_{i\in I} P_i\right) & \subseteq & \bigcap\limits_{i\in I} P_i \end{array}$$

(ii) For any $\lambda \in R$ the eigenspace of φ to λ a sumbodule of M, that is invariant under φ, which means

$$\varphi\left(\mathrm{Eig}_\varphi(\lambda)\right) \quad \subseteq \quad \mathrm{Eig}_\varphi(\lambda)$$

And if M is torsion free [which is $ax = 0 \implies a = 0$ or $x = 0$], then any eigenspace $\mathrm{Eig}_\varphi(\lambda)$ even is a pure sub-module of M, that is for any $a \in R$ with $a \neq 0$ we get the implication

$$ax \in \mathrm{Eig}_\varphi(\lambda) \quad \implies \quad x \in \mathrm{Eig}_\varphi(\lambda)$$

Nota if R is a PID, then by (4.109.(ii)) this implies, that any eigenspace of φ is complemented, that is $M = \mathrm{Eig}_\varphi(\lambda) \oplus Q$ for some $Q \leq_{\mathsf{m}} M$. However, Q need not be φ-invariant again.

(iii) Let R be an integral domain and M be free and finitely generated. Then the spectrum of φ is precisely the set of roots of the polynomial function $R \to R : \lambda \mapsto \det(\varphi - \lambda \mathbb{1}_M)$, that is

$$\mathrm{Spec}(\varphi) \quad = \quad \{\, \lambda \in R \mid \det(\varphi - \lambda \mathbb{1}_M) = 0 \,\}$$

(iv) Let R be an integral domain and M be torsion-free, then eigenvectors to distinct eigenvalues are linearly independent: Given $\lambda_1, \ldots, \lambda_n \in R$ pairwise distinct elements [that is $\lambda_i = \lambda_j \implies i = j$] of R and $x_i \in \mathrm{Eig}_\varphi(\lambda_i)$ with $x_i \neq 0$ for any $i \in 1 \ldots n$ then $\{\, x_1, \ldots, x_n \,\}$ is linearly independent.

(v) More generally: If R is an integral domain, M is torsion-free and $\lambda_1, \ldots, \lambda_n \in R$ are pairwise distinct elements of R, again. Then we consider some subsets $U_i \subseteq \mathrm{Eig}_\varphi(\lambda_i)$ where $i \in 1 \ldots n$. If now all the U_i are linearly independent, then U is linearly independent as well:

$$U \quad := \quad \bigcup_{i=1}^{n} U_i \quad \subseteq \quad M$$

(5.38) Example:
Let $(R, +, \cdot)$ be an integral domain, fix $1 \leq n \in \mathbb{N}$ and consider the diagonal matrix D with entries $\lambda_1, \ldots, \lambda_n \in R$ and another matrix J which has $\lambda \in R$ on the diagonal and $1 \in R$ one step above

$$D \quad := \quad \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \lambda_n \end{pmatrix}, \quad J \quad := \quad \begin{pmatrix} \lambda & 1 & & 0 \\ & \lambda & \ddots & \\ & \ddots & \ddots & 1 \\ 0 & & & \lambda \end{pmatrix}$$

Then the spectrum of D is precisely $\mathrm{Spec}(D) = \{\, \lambda_1, \ldots, \lambda_n \,\}$, whereas J only has λ in its spectrum $\mathrm{Spec}(J) = \{\, \lambda \,\}$. And if $\{\, e_1, \ldots, e_n \,\}$ is the usual Euclidean basis of R^n then for any $\alpha \in R$ the eigenspace of α is given to be

$$\begin{aligned} \mathrm{Eig}_D(\alpha) \quad &= \quad \mathrm{Lh}\{\, e_i \mid i \in 1 \ldots n,\, \lambda_i = \alpha \,\} \\ \mathrm{Eig}_J(\lambda) \quad &= \quad R\, e_1 \end{aligned}$$

These are the two classic examples: D shows how neatly the eigenspaces of a diagonal matrix are arranged and J is an example of a matrix that cannot be diagonalized. These matrices J will later be called *Jordan-blocks*.

Prob Clearly $De_i = \lambda_i e_i$ such that any $e_i \in \mathrm{Eig}_D(\lambda_i)$ is an eigenvectors of D to the eigenvalue λ_i, in particular $\lambda_i \in \mathrm{Spec}(D)$. Conversely the equation $Dx = \alpha x$ breaks down into n equations in R, namely $\lambda_i x_i = \alpha x_i$ and hence $(\lambda_i - \alpha)x_i = 0$. So if $\alpha \notin \{\lambda_1, \ldots, \lambda_n\}$ then (as R is an integral domain) $x_i = 0$ for any $i \in 1 \ldots n$ and hence $x = 0$. Thus the λ_i are all the eigenvalues D has. The same reasoning shows that $Dx = \alpha x$ implies $x \in \mathrm{Lh}\{ e_i \mid i \in 1 \ldots n, \lambda_i = \alpha \}$ and the converse inclusion is clear.
Prob Clearly $Je_1 = \lambda e_1$ such that e_1 is an eigenvector of J to the eigenvalue λ. Conversely the equation $Jx = \alpha x$ breaks down into the equations $\lambda x_n = \alpha x_n$ and $\lambda x_i + x_{i+1} = \alpha x_i$ for any $1 \leq i < n$. Thus if $\alpha \neq \lambda$ then (since R is an integral domain) we have $x_n = 0$. Then the $(n-1)$-th equation is $\lambda x_{n-1} = \alpha x_{n-1}$ such that $x_{n-1} = 0$ as well. By induction we find that $x = 0$, such that λ is the one and only eigenvalue of J. The matrix $\lambda \mathbb{1}_n - J = -N$ has the entries -1 on the upper off-diagonal only. Hence $(\lambda \mathbb{1}_n - J)x = -(x_2, x_3, \ldots, x_n, 0)$. From this we see, that the kernel of $\lambda \mathbb{1}_n - J$ is precisely $R\, e_1$ and this is the eigenspace of J to the eigenvalue λ.

(5.39) Example:
Consider any commutative ring R, e.g. $R = \mathbb{Z}$ and the free R-module $M := R^3$ of dimension 3. The endomorphism $\varphi(a,b,c) := (2a, c, 0)$ has the following representation as a matrix (in the euclidean basis)

$$A \;=\; \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

Obviously $e_1 = (1,0,0)$ is an eigenvector of A, to the eigenvalue 2, as $Ae_1 = 2e_1$ and also e_2 is an eigenvector of A, to the eigenvalue 0, as $Ae_2 = 0e_2$ - generally $\mathrm{Eig}_\varphi(0) = \mathrm{kn}(\varphi)$. It is clear [e.g. be regarding the characteristic polynomial $c_\varphi(t) = t^2(t-2)$, see below] that 0 and 2 are the only eigenvalues of φ. Both eigenspaces are direct summands of M, as

$$R^3 \;=\; Re_1 \oplus Re_2 \oplus Re_3 \;=\; \mathrm{Eig}_\varphi(2) \oplus \mathrm{Eig}_\varphi(0) \oplus Re_3$$

However the complement Re_3 is *not* invariant under φ, as $Ae_3 = e_2 \in \mathrm{Eig}_\varphi(0)$. This example shows, that is well possible, that a vector outside an eigenspace can be sucked into an eigenspace (under φ). But once inside they remain trapped, regardless of how many times we apply φ.

(5.40) Remark:
If $(R, +, \cdot)$ is a commutative ring, $f \in R[t]$ is a polynomial and A an element of an R-algebra, in our case here $A \in \mathrm{mat}_n(R)$ a square matrix over R, then we defined the *evaluation* of f in A to be the following element of the R-algebra again:

$$f(A) \;=\; \sum_{k=0}^{\infty} f[k] A^k \;\in\; \mathrm{mat}_n(R)$$

This is well-defined, as f has finite degree d, such that in truth the sum is finite only. More explicitly, if $f(t) = a_d t^d + \cdots + a_1 t + a_0$ then $f(A)$ is given to be

$$f(A) \;=\; a_d A^d + \cdots + a_1 A + a_0 \mathbb{1}_n$$

And if M is an R-module, then $\mathrm{end}(M)$ also is an R-algebra, under the composition of maps, for multiplication. Hence we may evaluate $f \in R[t]$ is an R-module endomorphism $\varphi \in \mathrm{end}(M)$, as well

$$f(\varphi) \;=\; \sum_{k=0}^{\infty} f[k]\varphi^k \;\in\; \mathrm{end}(M)$$

By construction of $R[t]$ the evaluation $R[t] \to \mathrm{end}(M) : f \mapsto f(\varphi)$ is a homomorphism of R-algebras. For convenience, if $f(t) = a_d t^d + \cdots + a_1 t + a_0$ again, then

$$f(\varphi) \;=\; a_d \varphi^d + \cdots + a_1 \varphi + a_0 \mathbb{1}_M$$

Recall that $\mathrm{mat}_n(R) \xrightarrow{\sim} \mathrm{end}(R^n) : A \mapsto \varphi_A$ is an isomorphism of R-algebras, where $\varphi_A(x) = Ax$. The inverse of this isomorphism is the basis representation $\mathrm{end}(R^n) \to \mathrm{mat}_n(R) : \varphi \mapsto [\varphi]_{\mathcal{E}}$, where $\mathcal{E}$ is the Euclidean basis of R^n. It is clear, that for any $x \in M$ and $k \in \mathbb{N}$ we have $\varphi_A^k(x) = A^k x$ and thereby $f(\varphi_A)(x) = f(A)x$. Generally, as $A \mapsto \varphi_A$ is an R-algebra homomorphism, it is clear that

$$f(\varphi_A) \;=\; \varphi_{f(A)}$$

(5.41) Definition:
Let $(R, +, \cdot)$ be a commutative ring and M be a free, finitely generated R-module. If now $\varphi \in \mathrm{end}(M)$ is an endomorphism of modules, then we introduce the following notions:

(i) For a square matrix $A = (a_{i,j}) \in \mathrm{mat}_n(R)$ over R we regard the following square matrix (of the same size) over the polynomial ring $R[t]$

$$t\mathbb{1}_n - A \;=\; \begin{pmatrix} t - a_{1,1} & -a_{1,2} & \cdots & -a_{1,n} \\ -a_{2,1} & t - a_{2,2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & -a_{n-1,n} \\ -a_{n,1} & \cdots & -a_{n,n-1} & t - a_{n,n} \end{pmatrix}$$

This is an $(n \times n)$-matrix over the polynomial ring $R[t]$ and thereby we define the **characteristic polynomial** $c_A(t)$ of A to be the determinant of this matrix

$$c_A(t) \;:=\; \det\big(t\mathbb{1}_n - A\big) \;\in\; R[t]$$

(ii) For an endomorphism $\varphi \in \mathrm{end}(M)$ we define the **characteristic polynomial** $c_\varphi(t)$ of φ using the following construction: Choose any ordered basis $\mathcal{M} \subseteq M$ of M and let $A := [\varphi]_{\mathcal{M}}$ be the matrix representation of φ, then $c_\varphi(t)$ is taken to be

$$c_\varphi(t) \;:=\; c_A(t) \;\in\; R[t]$$

Prob We need to check that this is well-defined, that is if $\mathcal{M}$ and $\mathcal{M}'$ are any two ordered bases and $A = [\varphi]_{\mathcal{M}}$ and $A' = [\varphi]_{\mathcal{M}'}$ are the respective matrix representations, then we need to show $c_A(t) = c_{A'}(t)$. Yet by (4.42.(iii)) there is an invertible matrix $T \in \mathrm{mat}_n(R)$ such that $A' = TAT^{-1}$. And since $t\mathbb{1}_n$ commutes with any matrix of $\mathrm{mat}_n(R[t])$ we find $T(t\mathbb{1}_n - A)T^{-1} = Tt\mathbb{1}_nT^{-1} - TAT^{-1} = t\mathbb{1}_n - A'$. And as T is invertible in $\mathrm{mat}_n(R[t])$ as well (with the same inverse) (4.55.(ii)) implies that the determinants are equal

$$\begin{aligned} c_{A'}(t) &= \det(t\mathbb{1}_n - A') = \det(T(t\mathbb{1}_n - A)T^{-1}) \\ &= \det(T) \cdot \det(t\mathbb{1}_n - A) \cdot \det(T)^{-1} \\ &= \det(t\mathbb{1}_n - A) = c_A(t) \end{aligned}$$

(iii) Let $\lambda \in R$ be any scalar, then we define the **algebraic multiplicity** of λ in $\varphi \in \mathrm{end}(M)$ to be the largest natural number $m \in \mathbb{N}$ such that $(t-\lambda)^m$ divides the charakteristic polynomial of φ

$$\mathrm{AM}_\varphi(\lambda) := \max\Big\{ k \in \mathbb{N} \mid (t-\lambda)^k \mid c_\varphi(t) \Big\}$$

(iv) For any scalar $\lambda \in R$ we also define the **geometric multiplicity** of λ in $\varphi \in \mathrm{end}(M)$ to be the rank of the eigenspace $\mathrm{Eig}_\varphi(\lambda) = \{ x \in M \mid \varphi(x) = \lambda x \}$ of φ to the eigenvalue λ

$$\mathrm{GM}_\varphi(\lambda) := \mathrm{rank}\Big(\mathrm{Eig}_\varphi(\lambda)\Big)$$

(v) Let R be an integral domain and M an arbitrary R-module: The **minimal polynomial** of $\varphi \in \mathrm{end}(M)$ is the uniquely determined polynomial that satisfies the following three properties - refer to (5.40) for details on $f(\varphi)$ and note, that generally φ might not have a minimal polynomial, at all

(1) $m_\varphi(\varphi) = 0$

(2) m_φ is monic

(3) $\forall f \in R[t] : f(\varphi) = 0 \implies m_\varphi \mid f$

Prob Suppose $m_1(t)$ and $m_2(t)$ satisfy the above three properties. In particular, as $m_2(\varphi) = 0$ we have $m_1 \mid m_2$. Likewise $m_1 \mid m_2$ and as R is an integral domain this yields $m_1 = am_2$ for some $a \in R[t]^* = R^*$. But as both are monic we can compare coefficients to find $m_1 = m_2$.

(5.42) Proposition: (viz. 976)
If $(R, +, \cdot)$ is an integral domain, M is an R-module and $\varphi \in \mathrm{end}(M)$ is an endomorphism of M, then we get the following statements concerning the minimal polynomial of φ

(i) The set $\{ f \in R[t] \mid f(\varphi) = 0 \}$ is an ideal of $R[t]$, called the *null ideal* of φ. In fact it is the kernel of the evaluation homomorphism $R[t] \to \mathrm{end}(M) : f \mapsto f(\varphi)$, that is

$$\{ f \in R[t] \mid f(\varphi) = 0 \} = \mathrm{kn}\big(f \mapsto f(\varphi)\big) \trianglelefteq_{\mathrm{i}} R[t]$$

(ii) If M is free and finitely generated and the null ideal of φ is a principal ideal then there also is a monic polynomial $m_\varphi \in R[t]$ that generates it, and in this case m_φ is the minimal polynomial of φ

$$m_\varphi R[t] \;=\; \{\, f \in R[t] \mid f(\varphi) = 0 \,\}$$

(iii) There are several equivalent formulations of whether a polynomial $m \in R[t]$ is the minimal polynomial $m = m_\varphi$ of φ: That is the following three statements are equivalent

(a) The polynomial m satisfies: (1) m is monic, (2) $m(\varphi) = 0$ and (3) for any $f \in R[t]$ we find that $f(\varphi) = 0$ implies $m \mid f$.

(b) The polynomial m satisfies: (1) m is monic, (2) $m(\varphi) = 0$ and (3) for any $f \in R[t]$ with $f \neq 0$ we find that $f(\varphi) = 0$ implies $\deg(m) \leq \deg(f)$.

(c) The polynomial m satisfies: (1) m is monic and (2) m generates the null ideal of φ, formally that is: $mR[t] = \{\, f \in R[t] \mid f(\varphi) = 0 \,\}$.

(iv) The null ideal $\mathfrak{v}_\varphi := \{\, f \in R[t] \mid f(\varphi) = 0 \,\}$ is a prime ideal of the polynomial ring $R[t]$ and if m is the minimal polynomial of φ, then m is a prime element of the polynomial ring $R[t]$.

(v) If $P \leq_{\mathsf{m}} M$ is a φ-invariant sub-module, that is $\varphi(P) \subseteq P$ again, and $\varphi \mid P : P \to P$ denotes the restriction of φ to P, then - supposed the minimal polynomials of φ and $\varphi \mid P$ exist - we find the following divisibility relation

$$m_{\varphi|P} \;\mid\; m_\varphi$$

(5.43) Example: (viz. 962)

(i) If $A = a\mathbb{1}_n$, that is A is the matrix belonging to $\varphi(x) = ax$ for some $a \in R$, then the minimal polynomial of A is $m_A(t) = t - a$, as clearly $m_A(A) = 0$ already. And for the characteristic polynomial of A we find $c_A(t) = (t-a)^n$, as the multi-linearity of the determinant yields

$$\det(t\mathbb{1}_n - a\mathbb{1}_n) \;=\; \det\big((t-a)\mathbb{1}_n\big) \;=\; (t-a)^n \det(\mathbb{1}_n) \;=\; (t-a)^n$$

(ii) More generally: If $A = \mathrm{dia}(a_1, \ldots, a_n)$ is a diagonal matrix, let λ_i be the distinct elements among the a_j. That is $\{\, \lambda_1, \ldots, \lambda_r \,\} = \{\, a_1, \ldots, a_n \,\}$ and $\lambda_i = \lambda_j$ is true for $i = j$ only. Also let $k(i)$ be the number of occurrences of λ_i among the a_j, that is $k(i) := \#\big\{\, j \in 1 \ldots n \mid a_j = \lambda_i \,\big\}$. If R is a commutative ring, then we find c_A and if R even is a noetherian integral domain we also find m_A

$$\begin{aligned} c_A(t) &= \prod_{i=1}^{r} (t - \lambda_i)^{k(i)} \\ m_A(t) &= \prod_{i=1}^{r} (t - \lambda_i) \end{aligned}$$

(iii) If $T = (t_{i,j}) \in \mathrm{tri}_n(R)$ is an upper (or lower) triangular matrix, then the characteristic polynomial of T splits into the linear factors $t - t_{ii}$, where $t_{i,i}$ is an element on the diagonal of T

$$c_T(t) \;=\; \prod_{i=1}^{n} (t - t_{i,i})$$

(iv) An easy example is the general 2×2 matrix A, that has the rows (a, b) and $(c, d) \in R^2$. For this matrix the characteristic polynomial is

$$\det \begin{pmatrix} t-a & -b \\ -c & t-d \end{pmatrix} \;=\; (t-a)(t-d) - bc \;=\; t^2 - (a+d)t + ad - bc$$

(v) If $A \in \mathrm{mat}_n(R)$ is any square matrix and A^* is the transpose of A, then both A and A^* share the same characteristic polynomial, since

$$\begin{aligned} c_{A^*}(t) &= \det(t\mathbb{1}_n - A^*) \;=\; \det((t\mathbb{1}_n - A)^*) \\ &= \det(t\mathbb{1}_n - A) \;=\; c_A(t) \end{aligned}$$

(vi) For a monic polynomial $f \in R[t]$ of degree $n := \det(f)$ let us introduce the **companion matrix** of f to be the following $n \times n$ square matrix

$$\mathrm{comp}(f) \;:=\; \begin{pmatrix} 0 & 0 & \cdots & 0 & -f[0] \\ 1 & 0 & \cdots & 0 & -f[1] \\ 0 & 1 & \cdots & 0 & -f[2] \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -f[n-1] \end{pmatrix} \;\in\; \mathrm{mat}_n(R)$$

For example let us present the companion matrix of the polynomial $f(t) = t^2 + at + b$ and compute its characteristic polynomial

$$\begin{aligned} \mathrm{comp}(f) &= \begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix} \\ \det \begin{pmatrix} t & b \\ -1 & t+a \end{pmatrix} &= t(t+a) + b \;=\; t^2 + at + b \end{aligned}$$

Note that the Euclidean basis $\{ e_1, e_2, \ldots, e_n \}$ is cycled in the following way: $\mathrm{comp}(f)e_k = e_{k+1}$ for any $1 \leq k < n$ and $\mathrm{comp}(f)e_n = -(f[0], f[1], \ldots, f[n-1])$. But more importantly both, the characteristic polynomial and the minimal polynomial of $\mathrm{comp}(f)$ are f again:

$$c_{\mathrm{comp}(f)}(t) \;=\; m_{\mathrm{comp}(f)}(t) \;=\; f(t)$$

(5.44) Lemma: (viz. 963) **Cayley-Hamilton Theorem**

(i) Let $(R, +, \cdot)$ be commutative ring and $A \in \mathrm{mat}_n(R)$ be an $n \times n$ matrix over R. Then the characteristic polynomial $c_A(t) = \det(t\mathbb{1}_n - A) \in R[t]$ is a monic polynomial of degree n over R, whose coefficients are given to be

$$c_A(t) \;=\; t^n - \mathrm{tr}(A)t^{n-1} + \cdots + (-1)^n \det(A) \;\in\; R[t]$$

More generally the k-th coefficient $c_A[k]$ of $c_A(t)$ where $k \in 0 \ldots n-1$ is given to be $(-1)^k$ times the sum of all *prinicipal minors* of A of size $r = n - k$. That is we have the formula:

$$c_A(t) \;=\; t^n + \sum_{r=1}^{n} (-1)^r \left(\sum_{\alpha \in \mathrm{Asc}(r,n)} \det\big(A[\alpha \mid \alpha]\big) \right) t^{n-r}$$

(ii) If we regard $A \in \mathrm{mat}_n(R)$ as an endomorphism $A : R^n \to R^n$ by virtue of $A(x) = Ax$, then A satisfies its own characteristic polynomial, that is we have

$$c_A(A) \;=\; \sum_{k=0}^{n} c_A[k] A^k \;=\; 0 \;\in\; \mathrm{mat}_n(R)$$

(iii) If $(R, +, \cdot)$ is a commutative ring, M a free, finitely generated R-module and $\varphi \in \mathrm{end}(M)$ an R-module endomorphism of M, then φ satisfies its own characteristic polynomial

$$c_\varphi(\varphi) \;=\; \sum_{k=0}^{n} c_\varphi[k] \varphi^k \;=\; 0 \;\in\; \mathrm{end}(M)$$

(iv) If $(R, +, \cdot)$ is a commutative ring again, M is any finitely generated R-module and $\varphi : M \to M$ is an R-module endomorphism, then there is a polynomial $f(t) \in R[t]$ of $\deg(f) = \mathrm{rank}(M)$ such that φ satisfies f, formally that is

$$f(\varphi) \;=\; \sum_{k=0}^{\mathrm{rank}(M)} f[k] \varphi^k \;=\; 0 \;\in\; \mathrm{end}(M)$$

(v) If $(R, +, \cdot)$ is a commutative ring, $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ is an ideal of R, M is any finitely generated R-module and $\varphi : M \to M$ is an R-module endomorphism such that $\varphi(M) \subseteq \mathfrak{a}M$, then φ is integral over $\mathfrak{a}$. That is there are $n \geq 1$ and $a_0, \ldots, a_{n-1} \in \mathfrak{a}$ such that

$$\varphi^n + a_{n-1}\varphi + \cdots + a_1 \varphi + a_0 \mathbb{1} \;=\; 0 \;\in\; \mathrm{end}(M)$$

(5.45) Remark:

(i) The proof of the general formula in (5.44.(i)) is a technical ordeal. It is far easier to only prove the reduced formula $c_A(t) = t^n - \mathrm{tr}(A) + \cdots \pm \det(A)$ only, which can be done by induction on n. And actually the only property truly needed is the fact that $c_A(t)$ is a polynomial of degree n with $c_A(0) = \det(A)$. So the reader is actually better off to prove this by induction, as an exercise, than to work through the proof here.

(ii) The proof of (5.44.(ii)) also is more or less technical and relies heavily on Cramer's rule. But why do we need to prove this anyway? Isn't it obvious that $c_A(A) = \det(A\mathbb{1}_n - A) = \det(0) = 0$? Well yes, of course $\det(A\mathbb{1}_n - A) = \det(0) = 0 \in R$. What Cayley-Hamilton tell us, is that if we evaluate the polynomial c_A in A we obtain the zero-matrix $c_A(A) = 0 \in \mathrm{mat}_n(R)$ and this is quite a different story, as there are many matrices with zero-determinant, that are non-zero themselves!

(iii) From now on we have to be aware, that we have two different ways of evaluating a polynomial $f \in R[t]$: First of all we can compute $f(a) \in R$ for any $a \in R$, as we did before. But secondly we can now compute $f(\varphi) \in \mathrm{end}(M)$ for any $\varphi \in \mathrm{end}(M)$. A special case is $A \in \mathrm{mat}_n(R)$ where $M = R^n$. Not to distinguish between these two different notions may lead to misconceptions like the one we described in (ii). In particular $c_A(B)$ is *not* $\det(B\mathbb{1}_n - A)$ [unless $n = 1$], as the first is an element of $\mathrm{mat}_n(R)$ and the latter is an element of R.

(iv) Part (iv) of the Cayley-Hamilton theorem is proved indenpendently from part (iii). Of course, if M also is free, then we are done, by pointing out $f = c_\varphi$. But in (iv) we did not require M to be free. So we loose the information which polynomial f turns φ to 0, but still, there is one.

(v) If $c_A(0) = \det(A) \in R^*$ is invertible, then A is invertible. Using the Cayley-Hamilton theorem we always have the following equation

$$\begin{aligned} 0 &= c_A(A) = A^n + \sum_{r=1}^{n-1} c_A[r] A^r + \det(A)\mathbb{1}_n \\ &= A\left(A^{n-1} + \sum_{r=1}^{n-1} c_A[r] A^{r-1}\right) + \det(A)\mathbb{1}_n \end{aligned}$$

Thus if $\det(A)$ is invertible, this equation may be used to show, that the inverse even is a polynomial (of degree $n-1$) in A, namely we can compute A^{-1} by virtue of

$$A^{-1} = \frac{1}{\det(A)}\left(A^{n-1} + \sum_{r=0}^{n-2} c_A[r+1] A^r\right)$$

(5.46) Proposition: (viz. 977)

(i) Let $(R, +, \cdot)$ be a commutative ring, M an R-module and $\varphi \in \mathrm{end}(M)$ an R-module endomorphism. If now $x \in M$ such that $\varphi(x) = \lambda x$ for some $x \in R$, then for any polynomial $f \in R[t]$ we get

$$f(\varphi)(x) = f(\lambda)\, x$$

(ii) If $(E, +, \cdot)$ is a field and V is a finitely generated E-vector space, then any E-vector space endomorphism $\varphi \in \mathrm{end}(V)$ has a (uniquely determined) minimal polynomial m_φ.

(iii) If $(R, +, \cdot)$ is a normal domain (e.g. an UFD), M a finitely generated, free R-module and $\varphi \in \mathrm{end}(M)$ an endomorphism of R-modules, then φ has a (uniquely determined) minimal polynomial m_φ.

(iv) Let $(R, +, \cdot)$ be an integral domain, M a free, finitely generated R-module and $\varphi \in \mathrm{end}(M)$ be an R-module endomorphism. Then the characteristic polynomial c_φ and minimal polynomial m_φ (if it exists) share the same roots in R. That is for any $\lambda \in R$ we get the equivalences

(a) $\lambda \in \mathrm{Spec}(\varphi)$

(b) $c_\varphi(\lambda) = 0$

(c) $m_\varphi(\lambda) = 0$

(d) $\det(\varphi - \lambda \mathbb{1}_M) = 0$

(v) Let $(R, +, \cdot)$ be a PID, M a free, finitely generated R-module and $\varphi \in \mathrm{end}(M)$ be an R-module endomorphism. Then for any $\lambda \in \mathrm{Spec}(\varphi)$ the dimension of the eigenspace of φ to λ lies in between 1 and the algebraic multiplicity of λ

$$1 \leq \mathrm{GM}_\varphi(\lambda) \leq \mathrm{AM}_\varphi(\lambda)$$

(5.47) Remark: (■)
In fact (5.46.(iii)) can be extended a little: If R is a normal domain (that is an integral domain, that is integrally closed in its quotient field), then any square matrix over R has a minimal polynomial and vice versa. That is for an integral domain R the following three statements are equivalent:

(a) R is a normal domain

(b) For any $A \in \mathrm{mat}_n(R)$ the ideal $\{ f \in R[t] \mid f(A) = 0 \}$ of $R[t]$ is principal

(c) For any $A \in \mathrm{mat}_n(R)$ the ideal $\{ f \in R[t] \mid f(A) = 0 \}$ of $R[t]$ is generated by a monic polynomial

That (a) implies (c) is (iii) and has also been shown by W. C. Brown in his paper Null Ideals and spanning Ranks of Matrices (1998), whereas (b) implies (a) has been proved by S. Frisch in Integrally closed Domains, Minimal Polynomials and Null Ideals of Matrices (2004) and (c) implies (b) is trivial.

(5.48) Proposition: (viz. 984)
Let $(R, +, \cdot)$ be commutative ring and L, M and N be finitely generated, free R-modules. Then we get the following statements

(i) If $\varphi \in \mathrm{end}(M)$ is an endomorphism on M and $\Phi : M \xrightarrow{\sim} N$ is an isomorphism of R-modules then the characteristic polynomial of the transferred endomorphism $\psi := \Phi\varphi\Phi^{-1} \in \mathrm{end}(N)$ is unchanged

$$c_\psi(t) = c_\varphi(t)$$

If now $f \in R[t]$ is any polynomial, then $f(\psi) = \Phi f(\varphi)\Phi^{-1}$ and hence ψ has a minimal polynomial if and only if φ has a minimal polynomial. And in this case we also get:

$$m_\psi(t) = m_\varphi(t)$$

(ii) If $\varphi \in \mathrm{end}(M)$ and $P \leq_\mathrm{m} M$ is a free sub-module of M such that $\varphi(P) \subseteq P$ and M/P is free, too, then we denote the maps

$$\begin{array}{rcll} \varphi \mid P & : & P \to P & : x \mapsto \varphi(x) \\ \overline{\varphi} & : & M\big/_P \to M\big/_P & : x + P \mapsto \varphi(x) + P \end{array}$$

Thereby the characteristic polynomial of φ splits into the characteristic polynomials of $\varphi \mid P$ and $\overline{\varphi}$ and in particular the characteristic polynomial of the restriction $\varphi \mid P$ divides $c_\varphi(t)$

$$c_\varphi(t) = c_{\varphi|P}(t) \cdot c_{\overline{\varphi}}(t)$$

(iii) If $\varphi \in \mathrm{end}(M)$ again and M is the inner direct sum $M = P_1 \oplus \cdots \oplus P_r$ where for any $i \in 1 \ldots r$ the sub-module $P_i \leq_{\mathfrak{m}} M$ is free, finitely generated and $\varphi(P_i) \subseteq P_i$ then we denote the restrictions $\varphi_i := \varphi \mid P_i$ again. And thereby the characteristic polynomial of φ splits into

$$c_\varphi(t) \;=\; \prod_{i=1}^{r} c_{\varphi_i}(t)$$

(iv) *Theorem of Fitting*: If M is a free R-module of $\dim(M) = n$ and $\varphi \in \mathrm{end}(M)$ an endomorphism of M and $f_1, \ldots, f_n \in R[t]$ are any polynomials such that $f_i(\varphi) = 0$ for any $i \in 1 \ldots n$, then the characteristic polynomial of φ divides the product of the f_i, formally

$$c_\varphi \;\mid\; f_1 \cdot \ldots \cdot f_n$$

(v) Let $\lambda \in \mathrm{end}(L)$, $\mu \in \mathrm{end}(M)$ and $\nu \in \mathrm{end}(N)$. Further let $\varphi : L \to M$ and $\psi : M \to N$ be homomorphisms of R-modules. Suppose that the following diagram is commutative and that its rows are exact, then we get: $c_\mu(t) \;=\; c_\lambda(t) \cdot c_\nu(t)$

$$\begin{array}{ccccccccc}
0 \to & L & \xrightarrow{\varphi} & M & \xrightarrow{\psi} & N & \to & 0 \\
 & \downarrow \lambda & \circlearrowleft & \downarrow \mu & \circlearrowleft & \downarrow \nu & & \\
0 \to & L & \underset{\varphi}{\longrightarrow} & M & \underset{\psi}{\longrightarrow} & N & \to & 0
\end{array}$$

(vi) If $(S, +, \cdot)$ is another commutative ring and $\alpha : R \to S$ is a homomorphism of rings, then we turn S into an R-algebra using $as := \alpha(a)s$ for $a \in R$ and $s \in S$. If now $\varphi \in \mathrm{end}(M)$ then we regard the change of base rings $M_S := S \otimes M$ and $\varphi_S := S \otimes \varphi \in \mathrm{end}(M_S)$. If now

$$\widetilde{\alpha} \;:\; R[t] \;\to S[t] \;:\; \sum_{k=0}^{\infty} a_k t^k \;\mapsto\; \sum_{k=0}^{\infty} \alpha(a_k) t^k$$

Then the characteristic polynomial of the endomorphism φ_S changed to S is just the characteristic polynomial of φ mapped under $\widetilde{\alpha}$

$$c_{\varphi_S}(t) \;=\; \widetilde{\alpha}\left(c_\varphi(t)\right)$$

(5.49) Corollary: (viz. 992)
Let $(R, +, \cdot)$ is an integral domain and M is a free, finitely generated R-module of dimension $n := \dim(M)$. Consider an R-module endomorphism $\varphi \in \mathrm{end}(M)$ that has a minimal polynomial (e.g. if R is an UFD). Then the minimal polynomial divides the characteristic polynomial, which in turn divides the n-th power of the minimal polynomial

$$m_\varphi \;\mid\; c_\varphi \quad \text{and} \quad c_\varphi \;\mid\; m_\varphi^n$$

In particular the minimal polynomial m_φ and characteristic polynomial c_φ share the same prime factors: That is for any prime element $p \in R[t]$ we have $p \mid m_\varphi \iff p \mid c_\varphi$.

(5.50) Definition:
Let $(R,+,\cdot)$ be a commutative ring $1 \leq n \in \mathbb{N}$ and $A \in \mathrm{mat}_n(R)$ be a square matrix over R. Then A is said to be a **diagonal matrix**, iff for any $i \neq j \in 1 \ldots n$ we have $a_{i,j} = 0$. In other words there are some $\lambda_1, \ldots, \lambda_n \in R$ [namely $\lambda_i = a_{i,i}$] such that A is given to be

$$A \quad = \quad \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \lambda_n \end{pmatrix}$$

And A is said to be **diagonizable** iff there an invertible matrix $T \in \mathrm{gl}_n(R)$ such that TAT^{-1} is a diagonal matrix. Let now M be a free, finitely generated R-module, then an endomorphism $\varphi \in \mathrm{end}(M)$ is said to be **diagonizable** iff there is some ordered basis $\mathcal{M} \subseteq M$ of M such that the matrix representation $[\varphi]_{\mathcal{M}}$ of φ is a diagonal matrix.

$$\exists\, \mathcal{M} \subseteq M \text{ ordered basis of } M, \text{ such that } [\varphi]_{\mathcal{M}} \text{ is a diagonal matrix}$$

An entire set $\{ \varphi_i \mid i \in I \} \subseteq \mathrm{end}(M)$ of endomorphisms of M is said to be **simultaneously diagonizable** iff there is some ordered basis $\mathcal{M}$ of M, such that all matrix representations $[\varphi_i]_{\mathcal{M}}$ are diagonal matrices

$$\exists\, \mathcal{M} \subseteq M \text{ ordered basis of } M, \text{ such that } \forall\, i \in I \,:\, [\varphi_i]_{\mathcal{M}} \text{ is a diagonal matrix}$$

(5.51) Remark:
If $(R,+,\cdot)$ is an integral domain, M is a free, finitely generated R-module and $\varphi \in \mathrm{end}(M)$ a diagonizable endomorphism of M, the we will see next, that there is an R-basis $\{ m_1, \ldots, m_n \}$ of M, such that for any $j \in 1 \ldots n$ there is some $a_j \in R$, such that $\varphi(m_j) = a_j m_j$. Clearly, the matrix representation of φ in the ordered basis $\mathcal{M} := (m_1, \ldots, m_n)$ is diagonal

$$[\varphi]_{\mathcal{M}} \quad = \quad \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & a_n \end{pmatrix}$$

We have studied this situation before: In example (5.36) we have seen that for any $\lambda \in R$ the eigenspace of φ to λ is the following free, finitely generated sub-module of M

$$\mathrm{Eig}_{\varphi}(\lambda) \quad = \quad \mathrm{Lh}\{ m_j \mid j \in 1 \ldots n,\, a_j = \lambda \}$$

And in example (5.43.(ii)) we continued: Let λ_i be the distinct elements among the a_j again. That is $\{ \lambda_1, \ldots, \lambda_r \} = \{ a_1, \ldots, a_n \}$ and $\lambda_i = \lambda_j$ is true for $i = j$ only. Then by in (5.38) we know that

$$\mathrm{Spec}(\varphi) \quad = \quad \{ \lambda_1, \ldots, \lambda_r \}$$

And if $k(i)$ is the number of occurrences of λ_i among the a_j, that is $k(i) := \#\{ j \in 1 \ldots n \mid a_j = \lambda_i \}$, then

(for a general commutative ring R) we found the characteristic polynomial of φ to be

$$c_\varphi(t) \;=\; \prod_{i=1}^{r}(t-\lambda_i)^{k(i)}$$

And if R even is a noetherian integral domain, then in (5.43.(ii)) we have also been able to prove, that the minimal polynomial of φ is the much same, only without multiplicities

$$m_\varphi(t) \;=\; \prod_{i=1}^{r}(t-\lambda_i)$$

(5.52) Theorem: (viz. 988)
Let $(R,+,\cdot)$ be a commutative ring, M be a free, finitely generated R-module. Also let $\varphi \in \mathrm{end}(M)$ be an R-module endomorphism and $\mathrm{Spec}(\varphi) = \{\lambda_1,\ldots,\lambda_r\} \subseteq R$ be the spectrum of φ. Then the following statements are equivalent - recall that in this case φ is said to be *diagonizable*:

(a) There is a basis $\{m_1,\ldots,m_n\} \subseteq M$ (for some $n \in \mathbb{N}$) of M, such that for any $i \in 1\ldots n$ there is some $\lambda_i \in R$, such that $\varphi(m_i) = \lambda_i m_i$.

(b) There is an ordered basis $\mathcal{M} \subseteq M$ of M, such that the matrix representation $[\varphi]_{\mathcal{M}}$ of φ in $\mathcal{M}$ is a diagonal matrix, formally: $\exists\,\lambda_1,\ldots,\lambda_n \in R : [\varphi]_{\mathcal{M}} = \mathrm{dia}(\lambda_1,\ldots,\lambda_n)$.

(c) For any ordered basis $\mathcal{M} \subseteq M$ of M the matrix representation $[\varphi]_{\mathcal{M}}$ of φ in $\mathcal{M}$ is a diagonizable matrix, formally: $\exists\,\lambda_1,\ldots,\lambda_n \in R : [\varphi]_{\mathcal{M}} \approx \mathrm{dia}(\lambda_1,\ldots,\lambda_n)$.

If R even is an integral domain, then we may append this list of equivalences: In this case (d) and (e) are equivalent to the above statements (a) to (c), as well, where:

(d) For any $i \in 1\ldots r$ the eigenspace $\mathrm{Eig}_\varphi(\lambda_i)$ is a free sub-module of M and M is the sum of the eigenspaces of φ

$$M \;=\; \sum_{i=1}^{r}\mathrm{Eig}_\varphi(\lambda_i)$$

(e) For any $i \in 1\ldots r$ the eigenspace $\mathrm{Eig}_\varphi(\lambda_i)$ is a free sub-module of M and M is an inner direct sum of the eigenspaces of φ

$$M \;=\; \bigoplus_{i=1}^{r}\mathrm{Eig}_\varphi(\lambda_i)$$

By (5.51), if R is an integral domain, then (a) implies property (h) and (h) implies (f). Also, if R is a noetherian, normal domain, then (a) also implies (g). If R even is a field, the converse implications are true, as well: In case R is a field (f) to (h) are equivalent to the above statements (a) to (e), where:

(f) The sum of the dimensions of all the eigenspaces of φ equals the dimension of M, that is we have

$$\dim(M) \;=\; \sum_{i=1}^{r}\mathrm{GM}_\varphi(\lambda_i)$$

(g) The minimal polynomial of φ splits into distinct linear factors over R. These linear factors are then

given to be $t - \lambda_i$, where the λ_i are the distinct eigenvalues of φ. Altogether we get

$$m_\varphi \;=\; \prod_{i=1}^{r}(t-\lambda_i)$$

(h) The characteristic polynomial of φ splits over R and for any eigenvalue λ_i of φ the algebraic multiplicities $\mathrm{AM}_\varphi(\lambda_i) = k(i)$ and geometric multiplicities $\mathrm{GM}_\varphi(\lambda_i) = \dim(\mathrm{Eig}_\varphi(\lambda_i))$ coincide

$$c_\varphi(t) \;=\; \prod_{i=1}^{r}(t-\lambda_i)^{k(i)} \quad \text{where} \quad k(i) \;=\; \dim\bigl(\mathrm{Eig}_\varphi(\lambda_i)\bigr)$$

criteria to be diagonizable AW 4.4.30 bis 4.4.32 und 4.4.40 und 4.4.49 how to diagonalize a matrix + example simultaneous diagonalization AW 4.3.36 spectral projections
R integral domain, $\varepsilon \in \mathrm{rend}(R)$, $s : R^n \times R^n \to R$ sesqui-linear for with respect to ε $\varphi \in \mathrm{end}(M)$ symmetric, i.e. $s(\varphi(x), y) = s(x, \varphi(y))$ then for any $x \in \mathrm{Eig}\varphi(\lambda)$, $y \in \mathrm{Eig}\varphi(\mu)$ we have $\lambda = \varepsilon(\mu)$ or $s(x, y) = 0$
$R = \mathbb{R}$ then: A diagonizable iff $A = A^*$ $R = \mathbb{C}$ then: A diagonizable iff $A\overline{A} = \overline{A}A$
functional calculus $f(\varphi)$ für $f \in C(\mathbb{R})$

5.4 Normal Forms

The theory of diagonalization is powerful and beautiful. Yet not every matrix is diagonalizable, not even over $\mathbb{C}$. Hence we need to look at other useful representations of an endomorphism as a matrix. In general (over a field) we find the *rational canonical form*. This is a block diagonal form, in which every block is the companion matrix of a polynomial. In case the characteristic polynomial splits the rational canonical form turns into the *Jordan normal form*.
The rational canonical form is closely related to the invariant factor theorem. In fact, if E is a field, then $E[t]$ is a PID, such that a finitely generated module M over $E[t]$ can be decomposed into invariant factors. We will find both the minimal polynomial and the characteristic polynomial in terms of these factors. But in order to do so, we first have to turn M into a module over the polynomial ring:

(5.53) Definition: (viz. 973)
Let $(R,+,\cdot)$ be a commutative ring, $(M,+,\diamond)$ be an R-module and fix an R-module-endomorphism $\varphi \in \mathrm{end}(M)$. Then we turn M into a module $(M_\varphi,+,\curlywedge)$ over the polynomial ring $R[t]$ using the following construction: The base set of M_φ is just M again: $M_\varphi := M$. Also the addition $+$ on M_φ is just the addition $+$ of M. The new ingredient is another scalar multiplication $\curlywedge$ on M_φ defined by

$$\curlywedge \;:\; R[t] \times M_\varphi \to M_\varphi \;:\; (f,x) \mapsto f(\varphi)(x) \;=\; \sum_{k=0}^{\infty} f[k]\varphi^k(x)$$

Again we write $fx := f \curlywedge x = f(\varphi)(x)$. More explicitly: If $f \in R[t]$ is any polynomial over R, written as $f = a_n t^n + \cdots + a_1 t + a_0 \in R[t]$ and $x \in M_\varphi$ is any element of M_φ, then the scalar multiplication is

$$fx \;=\; f(\varphi)(x) \;=\; a_n\varphi^n(x) + \cdots + a_1\varphi(x) + a_0 x$$

Nota even though $M_\varphi = M$ is the same set and the addition $+$ is identical we have to distinguish M and M_φ because of the different base ring and scalar multiplication. And as we only write M_φ in place of $(M_\varphi,+,\curlywedge)$ we have no other option, as to adapt the name of the base set.

(5.54) Remark:
The above definition might look a little artificial, but in fact it is a most ingenious construction that links module theory to linear algebra. In fact the entire theory of canonical forms of an endomorphism (e.g. Jordan canonical form) will arise by applying the invariant factor theorem to this module. Hence it is worthwhile to linger here for a moment to reflect on what we just defined:

As we have seen in (3.71.(vii)) $(\mathrm{end}(M),+,\circ)$ is a (non-commutative) ring under the point-wise addition $\varphi+\psi : x \mapsto \varphi(x)+\psi(x)$ and the composition $\circ$ of maps as multiplication $\varphi\psi : x \mapsto \varphi(\psi(x))$. Thereby $R \subseteq \mathrm{end}(M)$ can be considered a sub-ring, using the embedding $a \hookrightarrow a\mathbb{1}_M$. If now $f = a_n t^n + \cdots + a_1 t + a_0 \in R[t]$ is any polynomial over R, then we can evaluate f in φ

$$f(\varphi) \;=\; a_n\varphi^n + \cdots + a_1\varphi + a_0\mathbb{1}_M \;\in\; \mathrm{end}(M)$$

Thereby $f(\varphi)$ is a well-defined endomorphism of M again. And the scalar multiplication on M_φ has then been defined by the action of $f(\varphi)$ on M, that is we have

$$fx \;=\; f(\varphi)(x) \;=\; a_n\varphi^n(x) + \cdots + a_1\varphi(x) + a_0x$$

Note that the image of the ring-homomorphism $R[t] \to \mathrm{end}(M) : f \mapsto f(\varphi)$ is the commutative sub-ring $R[\varphi]$ of $\mathrm{end}(M)$. And also we see that $fx = 0$ if and only if $f(\varphi)(x) = 0$ and thereby the annihilator of $x \in M_\varphi$ is the set of all polynomials f such that $f(\varphi)(x) = 0$, formally

$$\mathrm{ann}(x) \;=\; \{\, f \in R[t] \mid f(\varphi)(x) = 0 \,\}$$

And thereby the annihilator of the entire module M_φ is the set of all polynomials f such that $f(\varphi) = 0$ is the zero map $M \to M : x \mapsto 0$, formally again

$$\mathrm{ann}(M_\varphi) \;=\; \{\, f \in R[t] \mid f(\varphi) = 0 \,\}$$

(5.55) Proposition: (viz. 974)
Let $(R, +, \cdot)$ be a commutative ring and consider two R-modules M and N. Also let $\mu \in \mathrm{end}(M)$ and $\nu \in \mathrm{end}(N)$ be two endomorphisms on these. Then the following statements are true:

(i) The $R[t]$-sub-modules of M_μ are precisely the μ-invariant R-sub-modules of M. That is for any subset $P \subseteq M$ we find the equivalence

$$P \;\leq_{\mathsf{m}}\; M_\mu \quad\Longleftrightarrow\quad P \;\leq_{\mathsf{m}}\; M \text{ and } \mu(P) \;\subseteq\; P$$

(ii) The $R[t]$-linear maps from M_μ to N_ν are precisely the R-linear maps φ from M to N that commute with μ and ν. More formally we find, that

$$\mathrm{mhom}_{R[t]}(M_\mu, N_\nu) \;=\; \{\, \varphi \in \mathrm{mhom}_R(M,N) \mid \varphi\mu \;=\; \nu\varphi \,\}$$

(iii) Let $\varepsilon \in \mathrm{end}(M)$ be another endomorphism on M and $\Phi : M \to M$ be a map from M to itself. Then Φ is an isomorphism from M_ε to M_φ if and only if Φ is an automorphism of M that commutes with ε and φ. That is the following equivalence golds true

$$\Phi : M_\mu \xrightarrow{\sim} M_\varepsilon \quad\Longleftrightarrow\quad \Phi : M \xrightarrow{\sim} M \text{ with } \varepsilon = \Phi\mu\Phi^{-1}$$

(5.56) Proposition: (viz. 974)
Let $(R, +, \cdot)$ be a commutative ring, M be an arbitrary R-module and fix an R-module endomorphism $\varphi \in \mathrm{end}(M)$. Then we obtain the following statements:

(i) For any $x \in M$ the subset $R[t]x \subseteq M_\varphi$ is a φ-invariant sub-module of M (and of M_φ) for which we get the inclusion $Rx \subseteq R[t]x \leq_{\mathsf{m}} M_\varphi$. Explicitly $R[t]x$ is given to be

$$R[t]\,x \;=\; \mathrm{Lh}_R\{\, \varphi^k(x) \mid k \in \mathbb{N} \,\}$$

(ii) If $x \in M_\varphi$ and $f \in R[t]$ is a monic polynomial of degree $n := \deg(f)$ with $fx = 0$, then $R[t]x$ even is finitely generated, as an R-module, since

$$R[t]x \;=\; \mathrm{Lh}_R\{\, \varphi^k(x) \mid 0 \le k < n \,\}$$

(iii) If $P \;\le_{\mathrm{m}}\; M$ is an φ-invariant sub-module of M and $x \in P$, then $R[t]x \subseteq P$. And if P is generated as $P = \mathrm{Lh}\{\, p_i \mid i \in I \,\}$ then P is also generated by

$$P \;=\; \sum_{i\in I} R[t]\, p_i$$

(iv) If M is a finitely generated R-module, then M_φ is a finitely generated $R[t]$-torsion module and the rank of M_φ does not exceed the rank of M, formally

$$\mathrm{rank}_{R[t]}(M_\varphi) \;\le\; \mathrm{rank}_R(M)$$

(5.57) Proposition: (viz. 979)
Let $(R, +, \cdot)$ be a commutative ring and M be free R-module of finite dimension $n = \dim(M) < \infty$. If now $\varphi \in \mathrm{end}(M)$ is an endomorphism of M, then the following statements are true:

(i) For any $x \in M$ the following four statements are equivalent - and in this case x is said to be a **cyclic** vector for φ

(a) $M_\varphi \;=\; R[t]\, x$

(b) $M \;=\; \mathrm{Lh}_R\{\, \varphi^k(x) \mid k \in \mathbb{N} \,\}$

(c) $M \;=\; \mathrm{Lh}_R\{\, \varphi^k(x) \mid 0 \le k < n \,\}$

(d) $\{\, \varphi^k(x) \mid 0 \le k < n \,\}$ is a basis of M

(ii) If $x \in M$ is a cyclic vector of M_φ and we denote the ordered basis $\mathcal{M} = (x, \varphi(x), \ldots, \varphi^{n-1}(x))$ then there is a monic polynomial $f \in R[t]$ of degree n such that $fx = 0$ and

$$[\varphi]_{\mathcal{M}} \;=\; \mathrm{comp}(f)$$

(iii) If $\mathcal{M} = (x_1, x_2, \ldots, x_n)$ is an ordered basis of M such that $[\varphi]_{\mathcal{M}} = \mathrm{comp}(f)$ for some monic polynomial $f \in R[t]$ then we find the following isomorphy of $R[t]$-modules

$$R[t] \,\big/\, fR[t] \;\xrightarrow{\sim}\; M_\varphi \;:\; g + fR[t] \;\mapsto\; gx_1$$

(iv) Combining the three items above, we find the equivalence of the following properties (a) to (c). Thereby the polynomials f in (b) and (c) have to be the same.

(a) There is some $x \in M$ such that $x \in M_\varphi$ is a cyclic vector.

(b) There is an ordered basis $\mathcal{M}$ of M and a monic polynomial $f \in R[t]$ such that $[\varphi]_{\mathcal{M}} = \mathrm{comp}(f)$.

(c) There is an some monic polynomial $f \in R[t]$ of degree $\deg(f) = n$ such that we have an isomorphy of the following $R[t]$-modules

$$R[t] \Big/ {}_{fR[t]} \;\cong_{\mathfrak{m}}\; M_\varphi$$

(5.58) Corollary: (viz. 981)
Rational canonical Form: Let $(E, +, \cdot)$ be a field and V be a finite-dimensional E-vector-space. Also fix an endomorphism $\varphi \in \mathrm{end}(V)$ of V. Then we pick up the invariant ideals of the $E[t]$-module V_φ: That is there some elements $x_1, \ldots, x_r \in V$ such that

(1) $V \;=\; E[t]x_1 \oplus \cdots \oplus E[t]x_r$ and

(2) $\mathrm{ann}(x_1) \;\supseteq\; \ldots \;\supseteq\; \mathrm{ann}(x_r)$

For any $i \in 1 \ldots r$ pick up the monic generator $f_i \in E[t]$ of the annihilator ideal $\mathrm{ann}(x_i) = f_i E[t]$ and say $n(i) := \deg(f_i)$. Then $n(i) = \dim(E[t]x_i) \geq 1$, as well and we get the following statements:

(i) $f_1 \mid f_2$ and $f_2 \mid f_3$ and so on until $f_{r-1} \mid f_r$

(ii) $f_r = m_\varphi$ is the minimal polynomial of φ

(iii) $f_1 \cdot \ldots \cdot f_r = c_\varphi$ is the characteristic polynomial of φ

(iv) For any $i \in 1 \ldots r$ the E-subspace $E[t]x_i$ has the ordered basis $\mathcal{V}_i := (x_i, \varphi(x_i), \ldots, \varphi^{n(i)-1}(x_i))$. And if we take $\mathcal{V} := (\mathcal{V}_1, \ldots, \mathcal{V}_r)$ this is an ordered basis of V and the matrix representation of φ in this basis is the block-diagonal matrix of the companion matrices of the f_i, that is

$$[\varphi]_{\mathcal{V}} \;=\; \mathrm{comp}(f_1) \oplus \cdots \oplus \mathrm{comp}(f_r)$$

(5.59) Remark:
We continue with a field E, a finite-dimensional E-vector space V and a fixed endomorphism $\varphi \in \mathrm{end}(V)$. Suppose the characteristic polynomial c_φ splits, that is, there are some $\lambda_1, \ldots, \lambda_s \in E$ and powers $1 \leq n(1), \ldots, n(s) \in \mathbb{N}$ such that c_φ can be written, as

$$c_\varphi(t) \;=\; \prod_{j=1}^{s} (t - \lambda_j)^{n(j)}$$

As in (5.58) let $f_1, \ldots, f_r \in E[t]$ be the invariant factors of V_φ. By the above corollary we have $f_r = m_\varphi$ and $c_\varphi = f_1 \ldots f_r$ and generally the ascending chain of divisibilities $f_1 \mid f_2 \mid \ldots \mid f_r = m_\varphi \mid c_\varphi$. If c_φ splits, then the same is true for all its divisors. That is

$$f_i(t) \;=\; \prod_{j=1}^{s} (t - \lambda_j)^{k(i,j)}$$

for some $0 \leq k(i,j) \leq n(j)$. In particular m_φ has the algebraic multiplicities $1 \leq k(j) = k(r,j)$. The divisibilities dictate $k(1,j) \leq \cdots \leq k(r,j)$ and as the invariant factors f_1 to f_{r-1} have to fill the gap

between m_φ and c_φ we find the following equations for any $j \in 1 \ldots s$:

$$n(j) - k(j) \;=\; \sum_{i=1}^{r-1} k(i,j)$$

So what are these invariant factors f_i for $1 \leq i < r$?

(5.60) Proposition: (viz. 982)
Let $(R, +, \cdot)$ be any commutative ring and M be an R-module. Then we use *change of base rings* (3.158) and regard the R-module and $R[t]$-module $M_{R[t]} := R[t] \otimes M$.

(i) By (3.146.(v)) any element of $M_{R[t]}$ can be written in the following form, where $d \in \mathbb{N}$ and $x_k \in M$. And this representation is *unique* in the sense that the x_k thereby are uniquely determined

$$\sum_{k=0}^{d} t^k \otimes x_k$$

(ii) If M is a free R-module having the R-basis $\{ m_1, \ldots, m_n \}$ then by (3.160.(i)) $M_{R[t]}$ is a free $R[t]$-module, having the $R[t]$-basis $\{ \mathbf{1} \otimes m_1, \ldots, \mathbf{1} \otimes m_n \}$.

Now fix any endomorphism $\varphi \in \mathrm{end}(M)$ of R-modules. Then we introduce two well-defined homomorphisms $\Delta_\varphi : M_{R[t]} \to M_{R[t]}$ and $\pi_\varphi : M_{R[t]} \to M_\varphi$ of $R[t]$-modules by linear expansion of

$$\begin{aligned} \Delta_\varphi\big(f \otimes x\big) \;&:=\; (tf) \otimes x + f \otimes \varphi(x) \\ \pi_\varphi\big(f \otimes x\big) \;&:=\; fx \;=\; f(\varphi)(x) \end{aligned}$$

(iii) These maps now form an exact chain of homomorphisms of $R[t]$-modules (or R-modules, whatever you prefer). That is the following chain of π_φ after Δ_φ is exact

$$0 \;\to\; M_{R[t]} \;\to\; M_{R[t]} \;\to\; M_\varphi \;\to\; 0$$

(iv) Thereby, if $\{ m_i \mid i \in I \} \subseteq M$ generates M as an R-module, then $\{ t \otimes m_i - \mathbf{1} \otimes \varphi(m_i) \mid i \in I \}$ generates the kernel $\mathrm{kn}(\pi_\varphi) \leq_{\mathfrak{m}} M_{R[t]}$ as an $R[t]$-module.

(v) If M is a free, finitely generated R-module, then so is $M_{R[t]}$ by (ii). And in this case we find the characteristic polynomial of φ to be the determinant of Δ_φ

$$\det\big(\Delta_\varphi\big) \;=\; c_\varphi(t) \;\in\; R[t]$$

5.5 Number Fields

p-adic valuation (and metric) Konstuktion der p-adischen Zahlen $\mathcal{Q}_p$ und $\mathcal{Z}_p$ Satz von Ostrowski Satz von Frobenius

5.6 Solving linear ODEs

Chapter 6

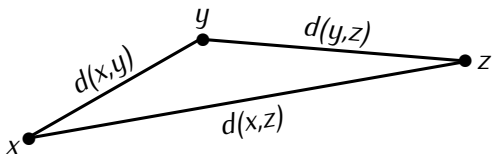
Functional Analysis

There are two ways of generalizing linear algebra of finite-dimensional vector-spaces: For one you can replace the base field by a (commutative) ring. This is what we did before in module theory. It turned out, that modules have a very rich structure and we have been able to classify finitely generated modules over PIDs.
The second generalisation you can think of is regarding non-finite vector-spaces. From a purely algebraic view, this is nothing new - the vector space still is of the form $E^{\oplus I}$ for some index set I with $|(|I)$ equal to its dimension. But that's not the end of the story: As always dropping a finiteness condition we need to replace it by some topology, in order to proceed. And we want to continue towards the spectral theory of bounded operators.
While unbounded operators are far more interesting in applications (quantum mechanics) they give rise to a theory that is based on measure, probability and integration theory. This has to be dealt with in a textbook similar to this one here. So what we do here is restrict ourselves to the base field of the real and complex numbers and venture on into the borderlands between linear algebra and analysis.

6.1 Metrics and Topologies

Both of these notions - metrics and topologies - are used to describe a notion of nearby or farther away, respectively. While metrics formalize the notion of distance in a very obvious way, topologies are a more abstract but very general concept. Truth is, both of these notions are native to analysis, as they are the prerequisites needed to define convergence. But it turned out, that topology is a very useful tool in algebra, too and there are instances, where you cannot proceed without.
We have tried to present an introduction into general topology in a very convincing way: We first introduce metrics and their properties and derive all the notions we use from topology from this case. In doing so, we try to enlighten the ideas, that lie at the bottom of the constructions in general topology.
So we want to measure distances: Say x and y are points in some space X. What properties do we expect from a function $d(x,y)$, that measures the distance between these points? Well, if $x = y$, then clearly $d(x,y) = 0$, otherwise not. Actually it is open to discussion, whether $d(x,y) = 0$ should imply $x = y$. We might want to drop this requirement, if our way of measuring a distance is less accurate, than the proximity of x and z. This happens in integration theory, where two functions can differ on a set of measure zero. But we will see, that this makes little difference.

The second property the distance $d(x,y)$ should satisfy is $d(x,y) = d(y,x)$. If this would not be satisfied, then the space in question would be non-isotropic: It would make a difference to go from x to y or the other way around. The last property is taken from plane geometry: Let fix x and z and place another point y somewhere in space. If y lies somewhere on the line xz from x to z, then $d(x,z) = d(x,y) + d(y,z)$. If y is somewhere else, then x, y and z form a triangle. And the side xz is shorter than the total of xy and yz. Therefore we get $d(x,z) < d(x,y) + d(y,z)$ in this case. In general we do not need the concept of a line in X, but we still retain the *triangle inequality* $d(x,z) \leq d(x,y) + d(y,z)$.



(6.1) Definition:
Let $X \neq \emptyset$ be any non-empty set. Then a function $d : X \times X \to \mathbb{R}$ is said to be a **metric** of X if it satisfies the following four properties for any x, y and $z \in X$

(M1) $d(x,y) \geq 0$

(M2) $d(x,y) = 0 \iff x = y$

(M3) $d(x,y) = d(y,x)$

(M4) $d(x,z) \leq d(x,y) + d(y,z)$

And in this case the ordered pair (X,d) is said to be a **metric space**. For any $r \in \mathbb{R}$ with $r > 0$ and any $x \in X$ let us then define the **open ball** of **radius** r to be the following subset $B_r(x)$ of X

$$B_r(x) := \{\, y \in X \mid d(x,y) < r \,\}$$

In case we want to emphasize the space X or metric d, under which the open ball $B_r(x)$ is taken, we also write $B_r(X,x)$ or $B_r(d,x)$ for this set. A general subset $U \subseteq X$ is said to be **open** iff any point $x \in U$ is contained in an open ball around x, that lies completely in U, formally

$$\forall\, x \in U \;\; \exists\, r > 0 \;:\; B_r(x) \subseteq U$$

(6.2) Example:

(i) On any non-empty set $X \neq \emptyset$, we can install the *trivial metric* by taking $d(x,x) := 0$ for any $x \in X$ and $d(x,y) := 1$ for any x, $y \in X$ with $x \neq y$. But as we can do this with any set, we cannot glean any information from it, which makes this metric rather worthless.

(ii) Probably the most well-known example is $X = \mathbb{R}^n$ or $X = \mathbb{C}^n$ respectively, introduced in (4.114). In this case we obtain the so-called *euclidean metric* on X by taking

$$d(x,y) := \sqrt{\sum_{k=1}^{n} (y_k - x_k)\,(\overline{y}_k - \overline{x}_k)}$$

where $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n) \in X$. Note that in case of $X = \mathbb{R}^n$ the sum runs over $(y_k - x_k)^2$ such that $d(x,y)$ is the pythagorean distance in n-dimensional space. This is a special case of the following situation: Any inner product on a complex vector-space V induces a norm and any norm induces a metric. This metric here is inherited from the inner product

$$\langle x \mid y \rangle \;=\; \sum_{k=1}^{n} x_k \overline{y}_k$$

(iii) Let $X := \mathbb{Z}$ and fix any prime number $p \in \mathbb{Z}$. Recall, that for any $a \in \mathbb{Z}$ with $a \neq 0$ we defined $\langle a \mid p \rangle = \max\{\, n \in \mathbb{N} \mid p^n \mid a \,\}$ and this is well-defined, as $\mathbb{Z}$ is an UFD. Then we obtain a metric d_p, called the *p-adic metric* on $\mathbb{Z}$, if for any $a, b \in \mathbb{Z}$ we let

$$d_p(a,b) \;:=\; \begin{cases} 0 \text{ if } a = b \\ \dfrac{1}{\langle b-a \mid p \rangle} \text{ if } a \neq b \end{cases}$$

Thereby properties (M1) to (M3) are immediately clear. For (M4) it is fairly easy to see, that for any three numbers a, b and $c \in \mathbb{Z}$ we have $\langle c-a \mid p \rangle \geq \min\{\, \langle b-a \mid p \rangle, \langle c-b \mid p \rangle \,\}$ and thereby $d_p(a,c) \leq \max\{\, d_p(a.b), d_p(b,c) \,\}$. This is an even stronger property, than (M4).

(6.3) Remark: (viz. 1185)
If $d : X \times X \to X$ satisfies (M1), (M3) and (M4) but only $x = y \implies d(x,y) = 0$, then d is said to be a **pseudo-metric** on X. In this case we obtain an equivalence relation on X, by letting

$$x \sim y \quad :\Longleftrightarrow \quad d(x,y) \,=\, 0$$

As always, if $Q := X/\sim$ denotes the quotient set of X under this relation, then mapping X to Q under $X \twoheadrightarrow Q : x \mapsto [x] = \{\, u \in X \mid d(u,x) = 0 \,\}$ is a natural way of how to replace X by Q. And in this case we obtain a well-defined metric on Q by letting

$$Q \times Q \;\to\; \mathbb{R} \;:\; \big([x],[y]\big) \;\mapsto\; d(x,y)$$

(6.4) Proposition: (viz. 1185)

(i) Consider a metric space (X,d) and x, $y \in X$ any two points in X. Also let $r > 0$, such that $y \in B_r(x)$. If we now take $\varepsilon := (r - d(x,y))/2$, then $B_\varepsilon(y) \subseteq B_r(x)$. In particular: If $P = B_r(x)$ is any open ball of X, then P already is an open subset of X.

(ii) Consider a metric space (X,d) and let $x \neq y \in X$ be two distinct points in X. Then there exist open subsets U, $V \subseteq X$, such that (1) $x \in U$, (2) $y \in V$ and (3) $U \cap V = \emptyset$.

(iii) Let (X,d) be a metric space, $X \neq \emptyset$ and consider any point $x \in X$ and $n \in \mathbb{N}$. For $n = 0$ we take $F_0(x) := X$ and for $n \geq 1$ let $F_n(x)$ be the open ball of radius $1/n$ around x. That is we define

$$F_n(x) \;:=\; B_{\frac{1}{n}}(x) \;=\; \left\{ y \in X \;\middle|\; d(x,y) < \frac{1}{n} \right\}$$

The collection $\mathcal{F}(x) := \{ F_n(x) \mid n \in \mathbb{N} \}$ is called the **local filter** of x. And the union of all local filters of X is called the **base of balls** $\mathcal{F} := \{ F_n(x) \mid x \in X, n \in \mathbb{N} \}$ of X. Then we get all of the following properties, for any $x \in X$ and $n \in \mathbb{N}$

(1) $x \in F_n(x)$ and the set $F_n(x) \subseteq X$ is open

(2) $\mathcal{F}(x)$ is a descending chain, that is $F_{n+1}(x) \subseteq F_n(x)$

(3) The intersection of $\mathcal{F}(x)$ is $\bigcap_n F_n(x) = \{ x \}$

(4) If $U \subseteq X$ is an open set and $x \in U$, then there is some $n \in \mathbb{N}$, such that $F_n(x) \subseteq U$

(5) If $x, y \in X$ with $x \neq y$, then there is some $n \in \mathbb{N}$ such that $F_n(x) \cap F_n(y) = \emptyset$

(6) We have $X \in \mathcal{F}$ and for any $x \in X$ and any $F, G \in \mathcal{F}$ such that $x \in F \cap G$ there is some $E \in \mathcal{F}$ such that $x \in E$ and $E \subseteq F \cap G$

(6.5) Definition:

(i) Let X be an arbitrary, non-empty set. Then an function x of the form $x : \mathbb{N} \to X$ is said to be a **sequence** in X. It is usual to denote $x_n := x(n)$ and $(x_n) := x$ in this case. Also, if $P \subseteq X$ is an arbitrary subset of X, then we write $(x_n) \subseteq P$ to abbreviate

$$\forall\, n \in \mathbb{N} \quad : \quad x_n \in P$$

(ii) If (x_n) and (y_n) both are sequences in X, then (x_n) is said to be a **sub-sequence** of (y_n) iff if there is some map $k : \mathbb{N} \to \mathbb{N}$ such that the following properties (1) to (3) are satisfied. And we abbreviate this by writing $(x_n) \subseteq (y_n)$.

(1) for any $n \in \mathbb{N}$ we get $n \leq k(n)$

(2) for any $m, n \in \mathbb{N}$ we get $m < n \implies k(m) < k(n)$

(3) for any $n \in \mathbb{N}$ we get $x_n = y_{k(n)}$

Nota It is obvious, then $\subseteq$ is both reflexive [that is $(x_n) \subseteq (x_n)$] and transitive [if $(x_n) \subseteq (y_n)$ and $(y_n) \subseteq (z_n)$ then $(x_n) \subseteq (z_n)$, as well], but it is *no* partial- order however, as it is *not* not anti-symmetric.

(iii) Let X be an arbitrary, non-empty set again. Then a binary relation $\to$ between the set $\mathcal{F}(\mathbb{N}, X)$ of sequences in X and elements of X is said to be a **convergence relation** on X, iff it satisfies the following three properties

(1) If (x_n) becomes *eventually constant*, that is there are some $N \in \mathbb{N}$ and some $x \in X$ such that for any $n \geq N$ we have $x_n = x$, then we have $(x_n) \to x$.

(2) The relation $\to$ is *right-unique*, that is for any sequence (x_n) and any $x, y \in X$ we get: If both $(x_n) \to x$ and $(x_n) \to y$ then already $x = y$.

(3) If (y_n) is a sequence in X, such that $(y_n) \to y$ for some $y \in Y$ and $(x_n) \subseteq (y_n)$ is a subsequence of (y_n), then we have $(x_n) \to y$, as well.

(6.6) Definition: (viz. 1186)
Let (X, d_X) be a metric space and $(x_n) \subseteq X$ be a sequence in X (refer to (6.5) above, for a definition and notations). Also let $x \in X$ be any element, then we say that (x_n) **converges** to x (and denote this by $(x_n) \to x$) iff satisfies the following property: If we draw an open ball around x - no matter how small - then from some index on the tail of (x_n) is contained in that open ball, entirely. Formally that is

$$\forall\, \varepsilon > 0 \;\; \exists\, n(\varepsilon) \in \mathbb{N} \;:\; \forall\, n \geq n(\varepsilon) \;:\; x_n \;\in\; B_\varepsilon(x)$$

Let (Y, d_Y) be another metric space and $f : X \to Y$ be a function. Then we say that f is **continuous** iff it satisfies one of the following three equivalent properties

(a) If $V \subseteq Y$ is open, then $f^{-1}(V) \subseteq X$ is open

(b) For any $x \in X$, $\varepsilon > 0$ there is some $\delta > 0$ such that $y \in B_\delta(X, x)$ implies $f(y) \in B_\varepsilon(Y, f(x))$.

(c) If $(x_n) \subseteq X$ is a sequence and $x \in X$ is a point such that $(x_n) \to x$ converges to x, then the image $(f(x_n)) \to f(x)$ converges to $f(x)$, as well.

(6.7) Definition:
If $X \neq \emptyset$ is a non-empty set and d and D are any two metrics on X, then d is said to be **coarser** or **laxer** than D (and in this case D is said to be **finer** or **stricter** than d), iff there is some $M \in \mathbb{R}$ with $M > 0$ such that for any x, $y \in X$ we get

$$d(x, y) \;\; \leq \;\; M \cdot D(x, y)$$

In this case we write $d \leq D$. Now d and D are said to be **equivalent** if both $d \leq D$ and $D \leq d$, written as $d \sim D$. In other words, there are m, $M > 0$ such that for any x, $y \in X$ we get

$$m \cdot D(x, y) \;\; \leq \;\; d(x, y) \;\; \leq \;\; M \cdot D(x, y)$$

Nota It is clear that $\sim$ is an equivalence relation on the set of all metrics on X. Also $\leq$ is a reflexive, transitive order on the set of all metrics on X and if $d \leq D$ and $D \leq d$, then clearly $d \sim D$.

(6.8) Proposition: (viz. 1187)
Let X be a non-empty set and d and D be two metrics on X, such that $d \leq D$, that is d is laxer than D. Then we get the following three properties:

(i) If for any x, $y \in X$ we have $d(x, y) \leq M \cdot D(x, y)$ for some $M > 0$, then for any $r > 0$ the open balls with respect to D are contained in open balls with respect to d. To be precise

$$B_{r/M}(D, x) \;\; \subseteq \;\; B_r(d, x)$$

(ii) Let $\mathcal{T}_d := \{\, U \subseteq X \mid \forall\, x \in U \, \exists\, r > 0 : B_r(d, x) \subseteq U \,\}$ be collection of all open subsets of X, with respect to the metric d. Likewise let $\mathcal{T}_D$ be the collection of all sets $U \subseteq X$, that are open with respect to the metric D. Then we get

$$\mathcal{T}_d \;\; \subseteq \;\; \mathcal{T}_D$$

(iii) If $(x_n) \subseteq X$ is any sequence in X that is convergent $(x_n) \to_D x$ with respect to the metric D for some $x \in X$, then (x_n) also is convergent $(x_n) \to_d x$ to x, with respect to the metric d, formally

$$(x_n) \to_D x \quad \Longrightarrow \quad (x_n) \to_d x$$

Topological Spaces

A metric d on a set X gives rise to open balls, which in turn give rise to the notions of convergence and of open subsets. We now want to regard both of these notions in a more general setting. Let us write down some properties we have found for open sets in metric spaces and try to pry further properties from them. This is what mathematicians do all the time and here this will be especially fruitful.

(6.9) Definition:

Let X be any set and let $\mathcal{T} \subseteq \mathcal{P}(X)$ be an arbitrary collection of subsets of X. Then $\mathcal{T}$ is said to be a **topology** of X and the ordered pair $(X, \mathcal{T})$ is said to be a **topological space**, iff $\mathcal{T}$ contains $\emptyset$ and X and is closed under finite intersections and arbitrary unions. That is $\mathcal{T}$ satisfies the following four properties

(T1) $\emptyset \in \mathcal{T}$

(T2) $X \in \mathcal{T}$

(T3) $U, V \in \mathcal{T} \implies U \cap V \in \mathcal{T}$

(T4) $\mathcal{U} \subseteq \mathcal{T} \implies \bigcup \mathcal{U} \in \mathcal{T}$

In this case the $U \in \mathcal{T}$ are said to be the **open** subsets of X. And a subset $C \subseteq X$ is said to be **closed**, iff its complement is an open set. As we consider $\mathcal{T}$ to be fixed on X, we denote this by writing

$$\begin{aligned} U \subseteq X \text{ open} \quad &:\Longleftrightarrow \quad U \in \mathcal{T} \\ C \subseteq X \text{ closed} \quad &:\Longleftrightarrow \quad X \setminus C \in \mathcal{T} \end{aligned}$$

For any $x \in X$ we finally denote the $\mathcal{T}(x) := \{ U \subseteq X \text{ open} \mid x \in U \}$ and call this the **neighbourhood system** of x. More generally, for an arbitrary subset $P \subseteq X$, we denote:

$$\mathcal{T}(P) \;:=\; \{ U \subseteq X \text{ open} \mid P \subseteq U \}$$

(6.10) Remark:

Let $(X, \mathcal{T})$ be a topological space and denote $\mathcal{Z} := \{ X \setminus U \mid U \in \mathcal{T} \}$ the collection of its closed subsets. Then $\mathcal{Z}$ is a family of subsets, that inherits properties dual to (T1) to (T4). In fact we get $\emptyset$ and $X \in \mathcal{Z}$ again and $\mathcal{Z}$ is closed under finite intersections and arbitrary intersections. That is for any $C, D \in \mathbb{Z}$, we also have $C \cup D \in \mathcal{Z}$ and for any subset $\mathcal{C} \subseteq \mathcal{P}(X)$ we get

$$\mathcal{C} \neq \emptyset \quad \Longrightarrow \quad \bigcap \mathcal{C} \in \mathcal{Z}$$

Prob clearly $\emptyset = X \setminus X$ and $X = X \setminus \emptyset$ are closed subsets of X. And if $C = X \setminus U$ and $D = X \setminus V \in \mathcal{Z}$, then $C \cap D = (X \setminus U) \cap (X \setminus V) = X \setminus (U \cap V)$ and as $U \cap V \in \mathcal{T}$ this means C, $D \in \mathcal{Z}$ again. Likewise if $\mathcal{C} = \{ C_i \mid i \in I \}$ for some $C_i = X \setminus U_i$, then $\bigcap \mathcal{C} = \bigcap_i C_i = \bigcap_i (X \setminus U_i) = X \setminus (\bigcup_i U_i)$ which is closed again, as $\bigcup U_i = \bigcup \{ U_i \mid i \in I \} \in \mathcal{T}$, since all the $U_i \subseteq X$ have been open.

(6.11) Example:

(i) Any set X carries two trivial topologies: For one the set $\{ \emptyset, X \}$ is a topology on X. It resembles the case that everything is clumped together, if $x \in X$ is a point, then X is the only open set that contains it. It is called the *indiscrete topology* on X, as it is the opposite of the next example.

(ii) On the other hand the set of *all* subsets $\mathcal{T} = \mathcal{P}(X)$ forms a topology on X - this is called the *discrete topology* on X and it resembles the situation there are absolutely no connections between any points x in X. As $\{x\}$ is an open set, every point $x \in X$ stands for itself and is not connected to any other point of X. Every two points of X even share the same distance, no matter what points you take. This is the topology induced by the trivial metric in (6.2.(i)): As any point $x \in X$ is is an open ball $\{x\} = B_{1/2}(x)$ any set $P \subseteq X$ is open, as P is the union of all its points.

(iii) If (X, d) is a metric space, then we find a topology on X, by declaring that a subset $U \subseteq X$ is open, iff every point $x \in U$ already has an open ball around it, that is contained in U. That is

$$U \subseteq X \text{ open} \quad :\Longleftrightarrow \quad \forall\, x \in U \;\; \exists\, r > 0 \;:\; B_r(x) \subseteq U$$

This is a special case of (6.12.(iii)), as the open balls in a metric space are a base of a topology. The latter has been proved as property (6) in (6.4.(iii)). Nota We use the convention, that any metric space is endowed this this topology, without specifically mentioning it.

(6.12) Lemma: (viz. 1188)

(i) Let $(X, \mathcal{T})$ be a topological space and $S \subseteq X$ be any subset. Then S inherits a topology $\mathcal{T} \cap S$ (called the *relative topology* of $\mathcal{T}$) by taking the open sets

$$\mathcal{T} \cap S \;:=\; \{ U \cap S \mid U \subseteq X \text{ open} \}$$

Nota and we use the convention, that any subset S of a topological space $(X, \mathcal{T})$ is automatically endowed with its relative topology, without specifically mentioning it.

(ii) Consider an arbitrary set X and a collection $\mathcal{Z} \subseteq \mathcal{P}(X)$ of subsets of X, that satisfies the following four properties [that are dual to properties (T1) to (T4) of a topology]

(C1) $\emptyset \in \mathcal{Z}$

(C2) $X \in \mathcal{Z}$

(C3) $C, D \in \mathcal{Z} \implies C \cup D \in \mathcal{Z}$

(C4) $\emptyset \neq \mathcal{C} \subseteq \mathcal{Z} \implies \bigcap \mathcal{C} \in \mathcal{Z}$

Then $\mathcal{Z}$ are the closed sets of a topology on X. That is we obtain a topology $\mathcal{T}$ on X by taking the complements of the sets of $\mathcal{Z}$ as open sets in X, formally

$$\mathcal{T} \;:=\; \{\, X \setminus C \mid C \in \mathcal{Z} \,\}$$

(iii) Consider an arbitrary set X and a collection $\mathcal{B} \subseteq \mathcal{P}(X)$ of subsets of X. Then $\mathcal{B}$ is said to be a **base** of a topology, iff it satisfies the following two properties

(B1) $X = \bigcup \mathcal{B}$

(B2) For any $x \in X$ and any $B, C \in \mathcal{B}$ such that $x \in B \cap C$ there is some $A \in \mathcal{B}$ such that $x \in A$ and $A \subseteq B \cap C$.

Then we obtain a topology $\mathcal{T}$ on X (called the topology *induced* by $\mathcal{B}$) by defining, that a subset $U \subseteq X$ is open, iff (a) any point $x \in U$ is contained in a base set $B \in \mathcal{B}$ that in turn is contained in U again or equivalently, iff (b) U is the union of some collection of base sets B_i (where I may be empty, finite or infinite). Formally that is

$$\begin{aligned} U \subseteq X \text{ open} \quad &:\Longleftrightarrow \quad \forall\, x \in U \;\; \exists\, B \in \mathcal{B} \;:\; x \in B \subseteq U \\ &\Longleftrightarrow \quad \exists\, \{\, B_i \mid i \in I \,\} \subseteq \mathcal{B} \text{ such that } U = \bigcup_{i \in I} B_i \end{aligned}$$

Nota If conversely $\mathcal{T} \subseteq \mathcal{P}(X)$ already is a topology on X and $\mathcal{B} \subseteq \mathcal{T}$ satisfies (one of) these properties (a) or (b), then we also get (B1), due to (T2) and (B2) due to (T3).

(iv) Let X be an arbitrary set and $I \neq \emptyset$ be a non-empty index-set. Suppose for any $i \in I$ we are given a topology $\mathcal{T}_i$ on X. Then their intersection $\mathcal{T} := \bigcap \mathcal{T}_i$ is a topology on X, as well.

Nota this allows us to define the topology on X generated by *any* subset of $\mathcal{P}(X)$, but it is much preferable to start with a basis of a topology, as in this case we get an explicit description of the topology, as we did in (iii).

(v) Let X and Y be any sets, where $(Y, \mathcal{T}_Y)$ is a topological space and consider a function $f : X \to Y$. Then we obtain a topology $f^{-1}(\mathcal{T}_Y)$ on X (called the *pull-back* of $\mathcal{T}_Y$) by defining

$$f^{-1}(\mathcal{T}_Y) \;:=\; \left\{ f^{-1}(V) \mid V \subseteq Y \text{ open} \right\}$$

(vi) Let I be any non-empty index set and for any $i \in I$ consider a topological space $(X_i, \mathcal{T}_i)$. Then we find a topology $\prod_i \mathcal{T}_i$ on the cartesian product set $\prod_i X_i$ (called the *box topology* of the $\mathcal{T}_i$) by defining that a subset V is open, iff any point $(x_i) \in V$ is contained in a set of the form $U := \prod_i U_i$ where $U_i \subseteq X_i$ is open for any $i \in I$, such that U is contained in V again, formally

$$V \subseteq \prod_{i \in I} X_i \text{ open} \quad :\Longleftrightarrow \quad \forall\, (x_i) \in V \;\; \exists\, (U_i) \;:\; U_i \subseteq X_i \text{ open and } (x_i) \in \prod_{i \in I} U_i \subseteq V$$

Nota and we use the convention, that the product space $\prod_i X_i$ is automatically endowed with the box topology $\prod_i \mathcal{T}_i$, without specifically mentioning it.

(6.13) Remark:
The relative topology of (6.12.(i)) makes the relation "is an open subset of" transitive. That is if $(X, \mathcal{T})$ is a topological space, $V \subseteq X$ is open and $U \subseteq V$ is open [in the sense of $(V, \mathcal{T} \cap V)$], then $U \subseteq X$ is open, as well. The same is true for the "is a closed subset of" relation. If $D \subseteq X$ is closed and $C \subseteq D$ is closed, then $C \subseteq X$ is closed, too.

Prob By definition $U \subseteq V$ is open, iff there is some $U' \subseteq X$ such that $U = U' \cap V$. As V is open and the intersection of two open sets is open again, we find $U \subseteq X$ to be an open subset of X. Likewise $C \subseteq D$ is closed, iff $C = D \setminus U$ for some $U \subseteq D$ open. That is $U = U' \cap D$ again and hence $C = D \setminus (U' \cap D) = D \setminus U' = D \cap (X \setminus U')$. Thus $C \subseteq X$ is closed, as D and $X \setminus U'$ are closed and the intersection thereby is closed, too.

(6.14) Remark:
In (6.12.(vi)) there is an alternate topology on the cartesian product $\prod_i X_i$ called the *product topology*. It is defined by using the following set as the base for the product topology

$$\mathcal{B} \;=\; \left\{ \prod_{i \in I} U_i \;\middle|\; \begin{array}{l} \forall\, i \in I : U_i \subseteq X_i \text{ open} \\ \#\{\, i \in I \mid U_i \neq X_i \,\} < \infty \end{array} \right\}$$

It is obvious that $\mathcal{B}$ is closed under finite intersections and thereby satisfies properties (1) and (2) in (6.12.(iii)). Thus V is an open set in the product topology iff it satisfies

$$V \subseteq \prod_{i \in I} X_i \text{ open} \quad :\Longleftrightarrow \quad \forall\, (x_i) \in V \;\; \exists \prod_{i \in I} U_i \in \mathcal{B} \text{ such that } (x_i) \in \prod_{i \in I} U_i \subseteq V$$

From this it is clear that in case of a finite set I the box topology equals the product topology. If I is infinite however, then the product topology only is a subset of the box topology (the box topology is *finer* than the product topology).

(6.15) Definition:
Let $(X, \mathcal{T})$ be a topological space and consider any subset $P \subseteq X$. Then we define the **interior** of P to be the largest open subset of X, that is contained in P, formally

$$P^\circ \;:=\; \bigcup \{\, U \subseteq X \text{ open} \mid U \subseteq P \,\} \;=\; \{\, x \in P \mid \exists\, U \subseteq X \text{ open} : x \in U \subseteq P \,\}$$

We will prove the equality of these sets (and all the other properties mentioned in this definition) in remark (6.16) below. Likewise we define the **closure** of P to be the smallest closed subset of X that contains P. That is we define

$$\overline{P} \;:=\; \bigcap \{\, C \subseteq X \text{ closed} \mid P \subseteq C \,\} \;=\; X \setminus \big(X \setminus P\big)^\circ$$

Then we have $P^\circ \subseteq P \subseteq \overline{P}$ and thereby we may define the **border** of P to be the closure of P without its interior - which is a closed subset of X. Formally again

$$\partial P \;:=\; \overline{P} \setminus P^\circ$$

(6.16) Remark: (viz. 1187)
Let $(X, \mathcal{T})$ be any topological space, and $P \subseteq X$ be any subset of X, then the identities for P° and $\overline{P}$ in definition (6.15) are true and we additionally obtain

(i) $P^\circ \subseteq X$ is open

(ii) $\overline{P} \subseteq X$ is closed

(iii) $\partial P \subseteq X$ is closed

(iv) $U \subseteq X$ is open, iff $U = U^\circ$

(v) $C \subseteq X$ is closed, iff $C = \overline{C}$

(vi) $P^\circ \subseteq P \subseteq \overline{P}$

(vii) $\overline{P} = P^\circ \cup \partial P$

(viii) If $C \subseteq X$ is closed and $P \subseteq C$, then $\overline{P} \subseteq C$

(ix) If for any $x \in V$ there is some $U \in \mathcal{T}(x)$ with $U \subseteq V$, then $V \subseteq X$ is open

(x) Let $S \subseteq X$ be any subset and regard S in the relative topology $\mathcal{T} \cap S$. If now $P \subseteq S$ is any subset we take $\mathrm{cl}_S(P)$ to be the closure of P in the relative topology $\mathcal{T} \cap S$ and $\mathrm{cl}_X(P)$ to be the closure of $P \subseteq X$ in the topology $\mathcal{T}$. And thereby we get

$$\mathrm{cl}_S(P) \;=\; \mathrm{cl}_X(P) \cap S$$

Nota the like statement for the interior of P is false, in general. As a counterexample regard $P = \{\, (x,0) \mid 0 \leq x < 1 \,\} \subseteq S$ where $S = \{\, (x,0) \mid x \in \mathbb{R} \,\}$ and $X = \mathbb{R}^2$. If we regard P as a subset of S, then the interior of P is given to be $\mathrm{it}_S(P) = \{\, (x,0) \mid 0 < x < 1 \,\}$ whereas for $P \subseteq X$ the interior is $\mathrm{it}_X(P) = \emptyset$.

Finiteness conditions are of great importance in algebra and analysis. The most common finiteness condition in topology is *compactness*. There is an entire world of notions and theorems concerning compactness and its relations to other properties, but as we are concerned with algebra, not analysis, we only introduce those notions we truly need.

(6.17) Definition:
Let $(X, \mathcal{T})$ be a topological space. Then a subset $K \subseteq X$ is said to be **compact** iff every open cover of K has a finite sub-cover. Formally: If $\{\, U_i \mid i \in I \,\} \subseteq \mathcal{T}$ is an arbitrary collection of open sets, then we get the following implication

$$K \subseteq \bigcup_{i \in I} U_i \quad \Longrightarrow \quad \exists\, \Omega \subseteq I \text{ finite, such that } K \subseteq \bigcup_{i \in \Omega} U_i$$

And a subset $P \subseteq X$ is said to be **precompact**, iff its closure $\overline{P} \subseteq X$ is a compact set. The topological space $(X, \mathcal{T})$ is said to be **compact**, iff the entire space X is compact. And $(X, \mathcal{T})$ is said to be **locally compact**, iff for every point $x \in X$ there is an open neighbourhood $U \in \mathcal{T}(x)$ such that $\overline{U}$ is a compact set.

(6.18) Proposition: (viz. 1190)

(i) If $(X, \mathcal{T})$ is a compact topological space and $C \subseteq X$ is a closed subset, then C is compact, as well.

(ii) If $(X, \mathcal{T})$ is any topological space and $K_1, \ldots, K_n \subseteq X$ are finitely many compact subsets of X, then the union $K_1 \cup \cdots \cup K_n$ of these sets is compact again.

(6.19) Definition:
Let $(X, \mathcal{T})$ be a topological space, then a function of the form $\mathcal{F} : \mathbb{N} \times X \to \mathcal{P}(X)$, that assigns any pair $(n, x) \in \mathbb{N} \times X$ a subset $F_n(x) := \mathcal{F}(n, x) \subseteq X$ is said to be a **system of local filters**, iff it satisfies the following four properties for any $n \in \mathbb{N}$ and any $x \in X$

(F1) $F_n(x) \in \mathcal{T}(x)$ is an open neighbourhood

(F2) The $F_n(x)$ form a descending chain: $F_{n+1}(x) \subseteq F_n(x)$

(F3) If $U \in \mathcal{T}(x)$, then there is some $n \in \mathbb{N}$ such that $F_n(x) \subseteq U$

(F4) For any $x, y \in X$ with $x \neq y$ there is an $n \in \mathbb{N}$, such that $F_n(x) \cap F_n(y) = \emptyset$

In this case the collection $\mathcal{F}(x) := \{ F_n(x) \mid n \in \mathbb{N} \} \subseteq \mathcal{T}$ is said to be the *local filter* of $\mathcal{F}$ at $x \in X$. Now, if $\mathcal{F}$ is a system of local filters, then we define a convergence relation [this will be proved in (6.21.(iii)] on X: If $(x_n) \subseteq X$ is a sequence and $x \in X$ is a point, then we define

$$(x_n) \to_{\mathcal{F}} x \quad :\Longleftrightarrow \quad \forall\, m \in \mathbb{N}\ \exists\, n(m) \in \mathbb{N}\ :\ \forall\, n \geq n(m)\ :\ x_n \in F_m(x)$$

Nota In a system of local filters $\mathcal{F}$ the sets $\mathcal{F}(x)$ are *not* filters in the sense of definition (6.22), not even prefilters, but chains ordered under inclusion $\subseteq$. And as such $\mathcal{F}(x)$ is what is called a *basis* of the neighbourhood filter $\mathcal{N}(x)$. That is $\mathcal{F}(x)$ gives rise to $\mathcal{N}(x)$ under the construction in (6.23.(iii)).

(6.20) Example:

(i) If (X, d) is a metric space, then we obtain a system of local filters on X, by taking $F_n(x) := B_{1/n}(x)$ as we have seen in (6.4.(iii)), properties (1), (2), (4) and (5). And the convergence relation on X, as a metric space, is precisely the convergence relation of this system of local filters. It can be rewritten as

$$\forall\, \varepsilon > 0\ \exists\, n(\varepsilon) \in \mathbb{N}\ :\ \forall\, n \geq n(\varepsilon)\ :\ d(x_n, x) < \varepsilon$$

(ii) Let $(R, +, \cdot)$ be a commutative ring and $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be an ideal, such that $\bigcap_n \mathfrak{a}^n = 0$. Then we obtain a system of local filters on R by letting $F_n(x) := x + \mathfrak{a}^n$. The topology on R thereby is called the **$\mathfrak{a}$-adic** topology, which is defined to be

$$U \subseteq R \text{ open} \quad :\Longleftrightarrow \quad \forall\, u \in U\ \exists\, n \in \mathbb{N}\ :\ u + \mathfrak{a}^n \subseteq U$$

Prob Clearly $x \in x + \mathfrak{a}^n$ and if $u \in x + \mathfrak{a}^n$ then $u - x \in \mathfrak{a}^n$. Thus $u + \mathfrak{a}^n = x + (u - x) + \mathfrak{a}^n = x + \mathfrak{a}^n$ such that $F_n(u) = F_n(x)$. In particular $F_n(x)$ is open and we have (F1). Now (F2) is clear from $\mathfrak{a}^{n+1} \subseteq \mathfrak{a}^n$ and (F3) is just the definition of the topology. For (F4) we consider $x \neq y$ and take $n \in \mathbb{N}$ such that $y - x \notin \mathfrak{a}^n$ which is possible, as $\bigcap \mathfrak{a}^n = 0$. If we then had $z \in (x + \mathfrak{a}^n) \cap (y + \mathfrak{a}^n)$ then $z - x \in \mathfrak{a}^n$ and $z - y \in \mathfrak{a}^n$ and thereby $y - x = (z - x) - (z - y) \in \mathfrak{a}^n$ too, a contradiction. Thus $(x + \mathfrak{a}^n) \cap (y + \mathfrak{a}^n) = \emptyset$, which is property (F4).

The next proposition studies the connection between topologies and systems of local filters. (6.21.(i)) tells us, that it is possible to reconstruct the topology $\mathcal{T}$ of X from the system of local filters $\mathcal{F}$. By (6.21.(vi)) we can even reconstruct the topology from the convergence relation induced by $\mathcal{F}$. However not all topological spaces admit a system of local filters and hence "topology" is the more general concept. (6.21.(ii)) classifies, which topologies admit a system of local filters - and which don't.

We need to fix a system of local filters on X to construct a convergence relation. However in (6.21.(iv)) it turns out, that the convergence relation actually does not depend on the specific system of filters $\mathcal{F}$ chosen. In this sense the convergence relation only depends on the underlying topology $\mathcal{T}$ on X. You might want to think of this in the following way: The absolute value of distance may be different, but the topology already determines, what is close by and what is far away and thereby convergence.
We will encounter this again in the setting of normed spaces. In a finite-dimensional normed space, all norms are equivalent and hence they all induce the same convergence relation. However, there are a multitude of norms out there, that induce different metrics.

(6.21) Lemma: (viz. 1190)

(i) If $(X, \mathcal{T})$ is a topological space and $\mathcal{F}$ is a system of local filters of X, then for an arbitrary subset $U \subseteq X$, the following two statements are equivalent

 (a) $U \subseteq X$ is open

 (b) For any $x \in U$ there is some $n \in \mathbb{N}$, such that $F_n(x) \subseteq U$

(ii) A topological space $(X, \mathcal{T})$ admits a system of local filters $\mathcal{F}$, if and only if the topology satisfies both of the following two properties

 (1) $(X, \mathcal{T})$ is a *Hausdorff-space*, that is for any two points $x, y \in X$ with $x \neq y$ there are open subsets $U, V \subseteq X$ such that $x \in U$ and $y \in V$, but $U \cap V = \emptyset$.

 (2) $(X, \mathcal{T})$ admits *countable neighbourhood bases*: For any $x \in X$ there is a set $\mathcal{B}(x) \subseteq \mathcal{T}(x)$ such that $\mathcal{B}(x)$ is countable and for any $U \in \mathcal{T}(x)$ there is some $B \in \mathcal{B}(x)$ such that $B \subseteq U$.

(iii) If $(X, \mathcal{T})$ is a topological space and $\mathcal{F}$ is a system of local filters of X, then we obtain a convergence relation $\to_{\mathcal{F}}$ on X by defining - for any sequence $(x_n) \subseteq X$ and point $x \in X$

$$(x_n) \to_{\mathcal{F}} x \quad :\Longleftrightarrow \quad \forall\, m \in \mathbb{N}\ \exists\, n(m) \in \mathbb{N} \,:\, \forall\, n \geq n(m) \,:\, x_n \in F_m(x)$$

(iv) If $(X, \mathcal{T})$ is a topological space and $\mathcal{E}$ and $\mathcal{F}$ are any two systems of local filters on X, then theses convergence relations are identical. That is for any sequence $(x_n) \subseteq X$ and $x \in X$, we get

$$(x_n) \to_{\mathcal{E}} x \iff (x_n) \to_{\mathcal{F}} x$$

Nota as the convergence relations actually do not depend on the specific system of local filters used, we will often omit the index $\mathcal{F}$ and write $(x_n) \to x$ only.

(v) If $(X, \mathcal{T})$ is a topological space, $\mathcal{F}$ is a system of local filters of X and $P \subseteq X$ is any subset, then closure of P is precisely the set of limits of convergent sequences in P, formally that is

$$\overline{P} = \left\{ x \in X \;\middle|\; \begin{array}{l} \exists\, (x_n) \subseteq P \text{ such that} \\ (x_n) \to_{\mathcal{F}} x \end{array} \right\}$$

(vi) If $(X, \mathcal{T})$ is a topological space, $\mathcal{F}$ is a system of local filters of X and $C \subseteq X$ is any subset, then the following two statements are equivalent

(a) $C \subseteq X$ is closed

(b) For any $(x_n) \subseteq C$ with $(x_n) \to_{\mathcal{F}} x$ we get $x \in C$

6.2 Continuous Maps

Filters are the next level of generalisation, when it comes to convergence. They are the right way to deal, with non-Hausdorff spaces. The general idea is, that the neighbourhood system $\mathcal{T}(x)$ is centred at x, that is in a Hausdorff space $(X,\mathcal{T})$ we always have $\bigcap \mathcal{T}(x) = \{ x \}$. In general this need not be true - just look at the indiscrete topology. The prototype of a filter is the neighbourhood filter $\mathcal{N}(x)$, introduced in (6.23.(i)). It also satisfies $\bigcap \mathcal{N}(x) = \{ x \}$ in a Hausdorff space. In general topology a filter $\mathcal{F}$ is said to converge $\mathcal{F} \to x$ against $x \in X$, iff $\mathcal{N}(x) \subseteq \mathcal{F}$, as in this case $\bigcap \mathcal{F} \subseteq \bigcap \mathcal{N}(x)$ which is thought to be the closest you can get towards a limit. As we will not need these concepts however, we will only scratch the surface, here.

(6.22) Definition:
Let X be any non-empty set, then a collection $\mathcal{F} \subseteq \mathcal{P}(X)$ of subsets of X is said to be a **prefilter**, iff it satisfies the following three properties

(1) $\mathcal{F} \neq \emptyset$ is non-empty

(2) for any $F \in \mathcal{F}$ we have $F \neq \emptyset$

(3) if $F \subseteq \mathcal{F}$ and $P \subseteq X$ is a arbitrary subset of X, then $F \subseteq P \implies P \in \mathcal{F}$ already

The latter property (3) is also known as the *upward closure property* of $\mathcal{F}$. And a prefilter that contains X and is also closed under finite intersections is said to be a **filter**. That is a filter $\mathcal{F}$ also satisfies

(1') $X \in \mathcal{F}$

(4) for any $E, F \in \mathcal{F}$ we have $E \cap F \in \mathcal{F}$, as well

(6.23) Proposition: (viz. 1192)

(i) If $(X,\mathcal{T})$ is any topological space and $x \in X$ is a point in X, then we obtain a filter $\mathcal{N}(x)$ - the so-called **neighbourhood-filter** of x - by letting

$$\mathcal{N}(x) \;:=\; \{ N \subseteq X \mid \exists\, U \in \mathcal{T}(x) : U \subseteq N \}$$

(ii) If $f : X \twoheadrightarrow Y$ is any surjective function between the sets X and Y and $\mathcal{F}$ is a (pre)filter on X, then the image $f(\mathcal{F}) := \{ f(F) \mid F \in \mathcal{F} \}$ is a (pre)filter on Y, again.

Nota This proposition includes: Given an arbitrary function $f : X \to Y$ we get a surjective function $f : X \twoheadrightarrow f(X)$. Thereby $f(\mathcal{F})$ is a (pre)filter on the image $f(X)$, but not necessarily on Y.

(iii) If X is any set, $x \in X$ is any point in X and $\mathcal{B} \subseteq \mathcal{P}(X)$ is a collection of subsets of X that satisfies (1) $\mathcal{B} \neq \emptyset$, (2) for any $B \in \mathcal{B}$ we get $x \in B$ and (3) for any $B, C \in \mathcal{B}$ there is some $A \in \mathcal{B}$ such that $A \subseteq B \cap C$, then we obtain a filter $\mathcal{F}$ on X, by letting

$$\mathcal{F} \;:=\; \{ F \subseteq X \mid \exists\, B \in \mathcal{B} : B \subseteq F \}$$

Nota if $\mathcal{F} = \{ F_n(x) \mid x \in X, n \in \mathbb{N} \}$ is a system of local filters on $(X, \mathcal{T})$ and $\mathcal{F}(x)$ is the local filter at $x \in X$, that is $\mathcal{F}(x) = \{ F_n(x) \mid n \in \mathbb{N} \}$, then it is plain to see that this construction yields the neighbourhood filter in (i). That is we get

$$\mathcal{N}(x) \;=\; \{ N \subseteq X \mid \exists\, n \in \mathbb{N} : F_n(x) \subseteq N \}$$

Continuous Maps

Homomorphisms φ respect the algebraic structure of the objects involved. E.g. we require $\varphi(x+y) = \varphi(x) + \varphi(y)$. Continuous functions f are the analogue of homomorphisms in topological spaces, as they respect the topological structure of the spaces involved. However the image of a function is hard to control, the preimage is far easier. Thus the standard definition of f being continuous requires $f^{-1}(V)$ to be an open set for any open set V. Yet there are lots of reformulations of this, (f) is probably the one that appeals best to the intuition of "nearby points remain nearby, when mapped under f".

(6.24) Definition: (viz. 1193)
Let $(X, \mathcal{T}_X)$ and $(Y, \mathcal{T}_Y)$ be any two topological spaces and consider a function $f : X \to Y$. Then f is said to be **continuous** ($\mathcal{T}_X$-$\mathcal{T}_Y$-continuous, to be precise), iff it satisfies one of the following seven equivalent properties (a) to (g)

(a) for any $V \subseteq Y$ open, we get $f^{-1}(V) \subseteq X$ open

(b) for any $D \subseteq Y$ closed, we get $f^{-1}(D) \subseteq X$ closed

(c) for any subset $Q \subseteq Y$, we get $f^{-1}\big(Q^\circ\big) \subseteq f^{-1}(Q)^\circ$

(d) for any subset $Q \subseteq Y$, we get $\overline{f^{-1}(Q)} \subseteq f^{-1}\big(\overline{Q}\big)$

(e) for any subset $P \subseteq X$, we get $f\big(\overline{P}\big) \subseteq \overline{f(P)}$

(f) for any $x \in X$ and $V \in \mathcal{T}\big(f(x)\big)$ there is some $U \in \mathcal{T}(x)$ such that $f(U) \subseteq V$

(g) For any $x \in X$ let us denote $\mathcal{N}(x) := \{ M \subseteq X \mid \exists\, U \in \mathcal{T}(x) : U \subseteq M \}$ the neighbourhood filter of $x \in X$ and $\mathcal{N}(f(x)) := \{ N \subseteq f(X) \mid \exists\, V \in \mathcal{T}(f(x)) : V \cap f(X) \subseteq N \}$ the neighbourhood filter of $f(x) \in f(X) \subseteq Y$. Then for any (pre)filter $\mathcal{F}$ on X we get the implication

$$\mathcal{N}(x) \subseteq \mathcal{F} \implies \mathcal{N}\big(f(x)\big) \subseteq f(\mathcal{F}) := \{ f(F) \mid F \in \mathcal{F} \}$$

(6.25) Proposition: (viz. 1195)
Let $(X, \mathcal{T}_X)$ and $(Y, \mathcal{T}_Y)$ be topological spaces and $f : X \to Y$ be any function. Also let $\mathcal{E} \subseteq \mathcal{T}_X$ be a local system of filters on X and $\mathcal{F} \subseteq \mathcal{T}_Y$ be a local system of filters on Y. Then the following three statements are equivalent

(a) $f : X \to Y$ is continuous

(b) for any $n \in \mathbb{N}$ and any $x \in X$ there is some $m \in \mathbb{N}$ such that $f(E_m(x)) \subseteq F_n(f(x))$

(c) for any $(x_n) \subseteq X$ and $x \in X$ we get $(x_n) \to_{\mathcal{E}} x \implies (f(x_n)) \to_{\mathcal{F}} f(x)$

It is worthwhile to compare the above proposition (6.25) to the case of metric spaces (6.6): We see that we have just found a direct generalization of continuous maps between metric spaces, to the case of topological spaces, that are hausdorff and have countable neighbourhood bases - these are precisely the topological spaces, that admit a system of local filters, according to (6.21.(ii)).

(6.26) Definition:
A map $\Phi : X \to Y$ is said to be a **homeomorphism** iff (1) it is bijective, (2) it is continuous and (3) the inverse map $\Phi^{-1} : Y \to X$ is continuous, too. Two topological spaces are said to be **homeomorphic**, iff there is a homeomorphism f from X to Y. In this case we write

$$(X, \mathcal{T}_X) \approx (Y, \mathcal{T}_Y) \quad :\Longleftrightarrow \quad \exists\, \Phi : X \to Y \text{ homeomorphism}$$

Nota the property of being homeomorphic is analogous to the concept of being isomorphic in algebra: If X and Y are homeomorphic, then the homeomorphism Φ transfers any topological property from X to Y and vice versa. Hence these spaces have identical topological properties, like being hausdorff, being compact, admitting a system of local filters and so on - you name it.

(6.27) Definition:
Let $(X, \mathcal{T}_X)$ and $(Y, \mathcal{T}_Y)$ be any topological spaces and consider any map $f : X \to Y$ between them. Then f is said to be **open**, iff it satisfies one of the following two equivalent properties

(a) for any $U \subseteq X$ open, the image $f(U) \subseteq Y$ is open

(b) for any $x \in X$ and any $U \in \mathcal{T}(x)$ we have $f(U) \in \mathcal{T}(f(x))$

Analogously, for any $x \in X$, let $\mathcal{Z}(x) := \{\, C \subseteq X \text{ closed} \mid x \in C \,\}$ denote the collection of closed sets containing x. Then f is said to be **closed**, iff it satisfies one of the following two equivalent properties

(a) for any $C \subseteq X$ closed, the image $f(U) \subseteq Y$ is closed

(b) for any $x \in X$ and any $C \in \mathcal{Z}(x)$ we have $f(C) \in \mathcal{Z}(f(x))$

Prob the direction (a) $\implies$ (b) is clear: If $U \in \mathcal{T}(x)$, then by (a) $f(U) \subseteq Y$ is open again. And whenever $x \in U$, then $f(x) \in f(U)$ is granted. Conversely for (b) $\implies$ (a): If $U = \emptyset$, then $f(U) = \emptyset$ is open again. And if $U \neq \emptyset$ then $U \in \mathcal{T}(x)$ for some $x \in X$. Thus by (b) $f(U) \in \mathcal{T}(f(x))$ and in particular $f(U)$ is open. For closed maps we can argue in exactly the same way.

(6.28) Example:

(i) Consider the function $f : \mathbb{R} \to \mathbb{R}$ where $f(x) := \mathrm{int}(x) = \max\{\, k \in \mathbb{Z} \mid k \leq x \,\}$. Then f is closed as its image is a subset of $\mathbb{Z} \subseteq \mathbb{R}$ which consists of discrete points. But it is not continuous, the preimage of $]0.5, 1.5[$ is $[1, 2[$ which is neither open nor closed.

(ii) The map $\pi_1 : \mathbb{R}^2 \to \mathbb{R} : (x, y) \to x$ is continuous and open (this will be proved below), but not closed. The hyperbola $H := \{\, (x, y) \in \mathbb{R}^2 \mid xy = 1 \,\}$ is closed in $\mathbb{R}^2$, as it is the preimage of $\{1\}$ of the continuous function $f(x, y) := xy$. But $\pi_1(H) = \mathbb{R}^*$ which is an open subset of $\mathbb{R}$.

(6.29) Proposition: (viz. 1195)

(i) If $(X, \mathcal{T}_X)$ and $(Y, \mathcal{T}_Y)$ are any topological spaces and $y_0 \in Y$ is a fixed point, then the constant map $X \to Y : x \mapsto y_0$ is continuous.

(ii) Let X be a non-empty set and $\mathcal{T}_1$ and $\mathcal{T}_2$ be topologies on X. We regard the identity $\mathbb{1}_X : X \to X$ as a map from $(X, \mathcal{T}_1)$ to $(X, \mathcal{T}_2)$, then $\mathbb{1}_X$ is $\mathcal{T}_1$-$\mathcal{T}_2$-continuous, if and only if $\mathcal{T}_2 \subseteq \mathcal{T}_1$.

(iii) If $(X, \mathcal{T}_X)$, $(Y, \mathcal{T}_Y)$ and $(Z, \mathcal{T}_Z)$ are topological spaces and $f : X \to Y$ and $g : Y \to Z$ are continuous functions, then the composition $gf : X \to Z$ is continuous again.

(iv) Let $(X, \mathcal{T}_X)$ and $(Y, \mathcal{T}_Y)$ be topological spaces, where $\mathcal{T}_Y$ is induced by the basis $\mathcal{B} \subseteq \mathcal{P}(Y)$, as defined in (6.12.(iii)). If now $f : X \to Y$ is a function, such that $f^{-1}(B) \subseteq X$ is open for any $B \subseteq \mathcal{B}$, then f already is continuous.

(v) Let $(X, \mathcal{T}_X)$ and $(Y, \mathcal{T}_Y)$ be topological spaces, where $\mathcal{T}_X$ is induced by the basis $\mathcal{A} \subseteq \mathcal{P}(X)$, as defined in (6.12.(iii)). If now $f : X \to Y$ is a function, such that $f(A) \subseteq Y$ is open for any $A \subseteq \mathcal{A}$, then f already is open.

(vi) Let $(X, \mathcal{T}_X)$ and $(Y, \mathcal{T}_Y)$ be topological spaces, where $\mathcal{T}_X$ is induced by the basis $\mathcal{A} \subseteq \mathcal{P}(X)$, as defined in (6.12.(iii)). If now $f : X \hookrightarrow Y$ is an injective function, such that $f(X \setminus A) \subseteq Y$ is closed for any $A \subseteq \mathcal{A}$, then f already is closed.

(vii) If $(X, \mathcal{T}_X)$ and $(Y, \mathcal{T}_Y)$ are topological spaces and $\Phi : X \to Y$ is any function, then the following three properties of Φ are equivalent

(a) Φ is a homeomorphism

(b) Φ is bijective, continuous and open

(b) Φ is bijective, continuous and closed

(viii) If $(X, \mathcal{T}_X)$ and $(Y, \mathcal{T}_Y)$ are any topological spaces, $K \subseteq X$ is a compact set and $f : X \to Y$ is a continuous map, then the image $f(K) \subseteq Y$ is a compact set, as well.

(ix) Let I be a non-empty index set and for any $i \in I$ let $(X_i, \mathcal{T}_i)$ be a topological space. We bestow the cartesian product $\prod_i X_i$ with the box or product topology (your choice). Then for any $j \in I$ the canonical projection π_j is both continuous and open

$$\pi_j \,:\, \prod_{i \in I} X_i \twoheadrightarrow X_j \,:\, (x_i) \mapsto x_j$$

(x) Let I be a non-empty index set and for any $i \in I$ let $(X_i, \mathcal{T}_i)$ be a topological space. We bestow the cartesian product $\prod_i X_i$ with the product topology. Fix any $j \in I$ and for any $i \in I$ with $i \neq j$ some $a_i \in X_i$. Then the embedding ι_j of X_j into the cartesian product is continuous, where

$$\iota_j \,:\, X_j \hookrightarrow \prod_{i \in I} X_i \,:\, x_j \mapsto \left(\begin{cases} x_j \text{ if } i = j \\ a_i \text{ if } i \neq j \end{cases} \right)$$

(xi) *Universal property of the product topology*: Let I be a non-empty index set and for any $i \in I$ let $(Y_i, \mathcal{T}_i)$ be a topological space. We bestow the cartesian product $\prod_i Y_i$ with the product topology. Also let $(X, \mathcal{T})$ be a topological space and for any $i \in I$ let $f_i : X \to Y_i$ be a continuous function. Then the product function $\prod_i f_i$ is continuous again, where

$$\prod_{i \in I} f_i \ : \ X \to \prod_{i \in I} X_i \ : \ x \mapsto \big(f_i(x)\big)$$

(6.30) Proposition: (viz. 1199)
Gluing Lemma: Let $(X, \mathcal{T}_X)$ and $(Y, \mathcal{T}_Y)$ be topological spaces and consider an arbitrary index set I. Suppose for any $i \in I$ we are given a subset $X_i \subseteq X$ such that X is covered by the X_i

$$X \ = \ \bigcup_{i \in I} X_i$$

Further suppose that for any $i \in I$ we are given continuous maps $f_i : X_i \to Y$ (where X_i is regarded in the relative topology $\mathcal{T}_X \cap X_i$) such that for any $i, j \in I$ we get

$$f_i\big|_{X_i \cap X_j} \ = \ f_j\big|_{X_i \cap X_j}$$

Then the functions f_i can be patched together to a single, well-defined function $f : X \to Y$ such that for any $i \in I$ we get $f_i = f\big|_{X_i}$ by virtue of

$$f \ : \ X \to Y \ : \ x \mapsto f_i(x) \quad \text{where} \quad x \in X_i$$

We now distinguish two variants: If (i) $X_i \subseteq X$ is open for any $i \in I$ or (ii) if I is finite and $X_i \subseteq X$ is closed for any $i \in I$ then the patchwork function f is continuous.

(6.31) Proposition: (viz. 1198)

(i) Let I be any non-empty index set and for any $i \in I$ consider a topological space $(X_i, \mathcal{T}_i)$. For any $i \in I$ let $f_i : X_i \to Y$ be an arbitrary map, to some fixed set Y. Then we can install a topology $\mathcal{T}_Y$ on Y, called the *final topology*, on Y by defining

$$V \subseteq Y \text{ open} \quad :\Longleftrightarrow \quad \forall\, i \in I \, : \, f_i^{-1}(V) \subseteq X_i \text{ open}$$

And thereby all the $f_i : X_i \to Y$ become continuous maps. Also, if $(Z, \mathcal{T}_Z)$ is another topological space and $g : Y \to Z$ is any map, then the following two statements are equivalent

(a) $g : Y \to Z$ is continuous

(b) $\forall\, i \in I$ the composition $gf_i : X_i \to Z$ is continuous

(ii) A special case of (i) is the *quotient topology*: If $(X, \mathcal{T})$ is any topological space and $\sim$ is an equivalence relation on X, then we can install a topology on the quotient set $X/\sim$ by defining

$$V \subseteq Y \text{ open} \quad :\Longleftrightarrow \quad \{\, x \in X \mid [x] \in V \,\} \subseteq X \text{ open}$$

That is the final topology induced by the canonical map $\varrho : x \mapsto [x]$, in particular ϱ is continuous. Also for any subset $P \subseteq X$ we get $\varrho^{-1}(\varrho(P)) = \bigcup \{ [p] \mid p \in P \}$. And thereby, for any $x \in X$ the equivalence class $[x] \subseteq X$ is open, iff the one-point set $\{ [x] \} \subseteq X/\sim$ is open:

$$[x] \subseteq X \text{ open} \iff \{ [x] \} \subseteq X/\sim \text{ open}$$

Nota A subset $P \subseteq X$ is said to be *saturated*, iff it is the union of some equivalence classes, i.e. iff $P = \bigcup \{ [p] \mid p \in P \}$. In this case we get $\varrho^{-1}(\varrho(P)) = P$. Therefore: If any open set $U \subseteq X$ already is saturated, then ϱ is an open map.

Connected Components

The aim of general topology is to generalize the concept of "nearby" in spaces in which there is no metric available. The concept if being "connected" is quintessential for this: Intuitively speaking a connected set is "all in one piece," without any separations or gaps. This is the formally correct way to speak of cohesion within a space and we will see that the propositions we derive match this intuition.

(6.32) Definition:

Let $(X, \mathcal{T})$ be any topological space and consider the subsets $X_i \subseteq X$ (where $i \in 1 \ldots n$) in the induced topology. Then X is said to be the **topological sum** of the X_i (which we denote by $X = X_1 \oplus \cdots \oplus X_n$) iff the X_i partition X and a subset $U \subseteq X$ is open if and only if any $U \cap X_i \subseteq X_i$ is open. Formally that is the X_i satisfy the following three properties

(1) $X = X_1 \cup \cdots \cup X_n$

(2) $\forall\, i \neq j \in 1 \ldots n \; : \; X_i \cap X_j = \emptyset$

(3) $\forall\, U \subseteq X$ we get $U \subseteq X$ open $\iff \big(\forall\, i \in 1 \ldots n : U \cap X_i \subseteq X_i \text{ open} \big)$

(6.33) Proposition: (viz. 1199)

(i) Suppose the topological space $(X, \mathcal{T})$ can be written as the topological sum $X = X_1 \oplus \cdots \oplus X_n$ for some subsets $X_i \subseteq X$. Then the X_i are both, open *and* closed subsets of X.

(ii) Let $(X, \mathcal{T})$ be any topological space and consider some subsets A, $B \subseteq X$, then we obtain the equivalence of the following statements

(a) $X = A \oplus B$

(b) $X = A \cup B$ and $\overline{A} \cap B = \emptyset = A \cap \overline{B}$

(c) A, $B \subseteq X$ are open and closed, $A \cap B = \emptyset$ and $A \cup B = X$

(iii) Consider some topological space $(X, \mathcal{T})$ containing the sets A, X_1 and $X_2 \subseteq X$ and for $i \in \{ 1, 2 \}$ let $A_i := X_i \cap A$. If X is the topological sum $X = X_1 \oplus X_2$ then A also is the topological sum $A = A_1 \oplus A_2$. Formally this is the implication

$$X = X_1 \oplus X_2 \implies A = A_1 \oplus A_2$$

(iv) Let $(X, \mathcal{T}_X)$ and $(Y, \mathcal{T}_Y)$ be any two topological spaces and consider a continuous map $f : X \to Y$. Further let $Y_1, Y_2 \subseteq Y$ be any subsets and for $i \in \{1,2\}$ let us denote $X_i := f^{-1}(Y_i)$. If now Y is the topological sum $Y = Y_1 \oplus Y_2$ then X also is the topological sum $X = X_1 \oplus X_2$. Formally this is the implication

$$Y = Y_1 \oplus Y_2 \quad \Longrightarrow \quad X = X_1 \oplus X_2$$

(6.34) Definition: (viz. 1200)
Let $(X, \mathcal{T})$ be an arbitrary topological space, then X is said to be **connected**, iff it satisfies one of the following equivalent conditions (a) to (d). A subset $C \subseteq X$ is said **connected**, iff it is connected in the relative topology, i.e. iff $(C, \mathcal{T} \cap C)$ is a connected topological space.

(a) The only subsets of X that are both, open and closed, are the trivial ones: $\emptyset$ and X.

(b) X cannot be decomposed as a non-trivial topological sum. That is for any two subsets $X_1, X_2 \subseteq X$ we get the implication $X = X_1 \oplus X_2 \implies X_1 = X$ or $X_2 = X$.

(c) If X is the union of *separated* subsets A and $B \subseteq X$ (that is $X = A \cup B$ and $\overline{A} \cap B = \emptyset = A \cap \overline{B}$) then we already get $A = X$ or $B = X$.

(d) If $A \subseteq X$ is a subset of X such that $A \neq \emptyset$ and $A \neq X$, then A has non-empty border $\partial A \neq \emptyset$.

(6.35) Proposition: (viz. 1200)
Let $(X, \mathcal{T}_X)$ be an arbitrary topological space and consider any two connected subsets C and $D \subseteq X$. Then we obtain the following statements

(i) If $A, B \subseteq X$ are any two subsets, with $C \subseteq A \cup B$ and $\overline{A} \cap B \cap C = \emptyset = A \cap \overline{B} \cap C$, then we already get $C \subseteq A$ or $C \subseteq B$.

(ii) If C and $D \subseteq X$ are connected subsets, such that the intersection $C \cap D \neq \emptyset$ is nonempty, then the union $C \cup D \subseteq X$ is connected, too.

(iii) More generally let $\mathcal{C} \subseteq \{ C \subseteq X \mid C \text{ connected} \}$ be a non-empty collection of connected subsets of X, that have non-empty intersection. Then their union is connected again

$$\mathcal{C} \neq \emptyset \text{ and } \bigcap \mathcal{C} \neq \emptyset \quad \Longrightarrow \quad \bigcup \mathcal{C} \subseteq X \text{ connected}$$

(iv) Consider a connected subset $C \subseteq X$ and an arbitrary subset $A \subseteq X$. Then we obtain the following implication

$$C \subseteq A \subseteq \overline{C} \quad \Longrightarrow \quad A \text{ connected}$$

(v) If $(Y, \mathcal{T}_Y)$ is any other topological space, $f : X \to Y$ is a continuous map and $C \subseteq X$ is a connected set in X, then the image $f(C) \subseteq Y$ is connected, too.

(6.36) Definition: (viz. 1201)
Let $(X, \mathcal{T})$ be an arbitrary topological space, then we obtain an equivalence relation $\sim$ on X by defining

$$x \sim y \quad :\Longleftrightarrow \quad \exists\, C \subseteq X \text{ connected } : \{ x, y \} \subseteq C$$

for any x, $y \in X$. The equivalence classes under this relation are said to be the **connected components** of X. And for any $x \in X$ we denote the connected component containing x by

$$\text{CNC}(x) \;:=\; [x] \;=\; \bigcup \{\, C \mid C \subseteq X \text{ connected } x \in C \,\}$$

We denote the quotient set of X under $\sim$ (that is the set of all connected components of X) by $\text{CNC}(X)$

$$\text{CNC}(X) \;:=\; X \big/ _{\sim} \;=\; \{\, \text{CNC}(x) \mid x \in X \,\}$$

(6.37) Proposition: (viz. 1201)
Let $(X, \mathcal{T})$ be a non-empty topological space and consider an arbitrary subset $A \subseteq X$ and a connected subset $X \subseteq X$. Then we obtain the statements

(i) If $K \in \text{CNC}(X)$ is a connected component of X, then K already is a closed, connected subset of X.

(ii) The connected components of X are precisely the maximal connected subsets of X. That is $K \subseteq X$ is a connected component iff it is a connected subset of X, such that for any other connected subset $C \subseteq X$ we get $K \subseteq C \implies K = C$. Put formally, that is

$$\text{CNC}(X) \;=\; \{\, C \subseteq X \mid C \text{ connected} \,\}^*$$

(iii) If $C \subseteq X$ is a connected subset, then there is a connected component $K \in \text{CNC}(X)$ such that $C \subseteq K$. And if $C \neq \emptyset$, then this K even is uniquely determined, formally

$$C \neq \emptyset, \text{ connected} \quad \Longrightarrow \quad \exists!\, K \in \text{CNC}(X) \,:\, C \subseteq K$$

(iv) In particular if X only has finitely many connected components, say $\text{CNC}(X) = \{\, K_1, \ldots, K_n \,\}$ for some $n \in \mathbb{N}$, then the connected components decompose X into a topological sum

$$X \;=\; K_1 \oplus \cdots \oplus K_n$$

Topological Groups
This is a textbook on algebra, not on general topology, so let's get back to algebra. The link between algebra and topology are topological groups - that are groups that also carry a topology and the group operations respect the topology. The theory is quite powerful: It takes little effort to generate topological groups, that are very well-behaved.

(6.38) Definition:
Let $(G,\circ)$ be any group and $\mathcal{T}$ be a topology on G. Then the triple $(G,\mathcal{T},\circ)$ is said to be a **topological group** iff the inversion map $\iota : G \to G : x \mapsto x^{-1}$ and for any x, $y \in G$ the composition maps λ_x (from left) and μ_x (from right) are continuous, where

$$\begin{aligned} \lambda_x &: G \to G : y \mapsto xy \\ \mu_y &: G \to G : y \mapsto xy \end{aligned}$$

Nota It is clear, that ι is self-inverse $\iota^{-1} = \iota$ and that $\lambda_x^{-1} = \lambda_{x^{-1}}$ respectively $\mu_y^{-1} = \mu_{y^{-1}}$. Thus, if $(G,\mathcal{T},\circ)$ is a topological group, then all these maps ι and all the λ_x and μ_y are continuous and hence even homeomorphisms (as their inverses are continuous, too).

(6.39) Proposition: (viz. 1203)
Let $(G,\circ)$ be any group and $\mathcal{T}$ be a topology on G. For any x, $y \in G$ regard the maps $\lambda_x : y \mapsto xy$ and $\mu_y : x \mapsto xy$ respectively. Also we regard the group composition map $\circ : G \times G \to G : (x,y) \mapsto xy$ where $G \times G$ is taken in the box (= product) topology. Then we obtain the equivalence of the following five statements:

(a) for any x, $y \in G$ the maps λ_x and $\mu : y$ are continuous

(b) the composition map $\circ : G \times G \to G : (x,y) \mapsto xy$ is continuous

(c) for any x, $y \in G$ and $U \subseteq G$ open, xU and $Uy \subseteq G$ are open, too

(d) for any x, $y \in G$ and $C \subseteq G$ closed, xC and $Cy \subseteq G$ are closed, too

(e) If $W \subseteq G$ is an open set and x, $y \in G$ are any elements satisfying $xy \in W$, then there are open neighbourhoods $U \in \mathcal{T}(x)$ and $V \in \mathcal{T}(y)$ such that for any $u \in U$ and $v \in V$ we have $uv \in W$.

(6.40) Remark:
If $(G,\circ)$ be any group and $\mathcal{T}$ is a topology on G, then in the light of proposition (6.39) we find the following set-theoretic description of a topological group: $(G,\mathcal{T},\circ)$ is a topological group, if and only if for any closed set $C \subseteq G$ we get the following statements

(1) for any $x \in G$ the coset $xC \subseteq G$ is closed

(2) for any $y \in G$ the coset $Cy \subseteq G$ is closed

(3) the set $C^{-1} := \{ x^{-1} \mid x \in C \} \subseteq G$ is closed

(6.41) Lemma: (viz. 1204)
Let $(G,+)$ be any commutative group and $(F_n) \subseteq \mathcal{P}(G)$ a sequence of subsets of G, that satisfy the following four properties (1) $F_0 = G$, (2) for any $n \in \mathbb{N}$ the set $F_n \leq_{\mathrm{g}} G$ is a subgroup, (3) for any $n \in \mathbb{N}$ we have the inclusion $F_{n+1} \subseteq F_n$ and (4) the intersection of all F_n is 0

$$\bigcap_{n\in\mathbb{N}} F_n = \{0\}$$

Then we obtain a metric d on G by letting $d(x,y) := 0$ for $x = y$ and for any $x, y \in G$ with $x \neq y$ we let

$$d(x,y) \;:=\; \frac{1}{2^n} \quad \text{where} \quad n \;:=\; \max\{\, k \in \mathbb{N} \mid x - y \in F_k \,\}$$

Thereby $x + F_n = \{\, y \in G \mid d(x,y) \leq 2^{-n} \,\}$ for any $n \in \mathbb{N}$. And if $\mathcal{T}$ is the topology on G induced by this metric, then $(G, \mathcal{T}, +)$ is a topological group. Thereby, for a subset $U \subseteq G$ the following three statements are equivalent

(a) $U \subseteq G$ is open

(b) $\forall\, x \in U : \exists\, r > 0 : B_r(x) \subseteq U$

(c) $\forall\, x \in U : \exists\, n \in \mathbb{N} : x + F_n \subseteq U$

Nota actually the exact values 2^{-n} of the metric are irrelevant. You might as well choose $1/(n+1)$ or most anything else. Generally speaking you can take $d(x,y) = \delta(n)$ for some function $\delta : \mathbb{N} \to \mathbb{R}$ that satisfies (1) $\delta(n) > 0$, (2) for any $n \in \mathbb{N}$ we have $\delta(n+1) < \delta(n)$ and (3) $(\delta(n)) \to 0$.

6.3 Banach Spaces

normed space sub-multiplicative norm
vector metrics $(x_n) \to x$ and $(y_n) \to y$ then $(ax_n) \to ax$ and $(x_n + y_n) \to x + y$ linear metrics $d(ax, ay) = |a|d(x, y)$ and $d(x, z) \leq d(x, y) + d(y, z)$ are vector metrics
infinite sums by the sequence of partial sums infinite sums over arbitrary index sets def: Cauchy-sequence, completeness, completion
Banach space Banach algebra
Let $(E, \|\cdot\|_E)$ and $(F, \|\cdot\|_F)$ be any two normed spaces over field $\mathbb{F} = \mathbb{R}$ of real or $\mathbb{F} = \mathbb{C}$ complex numbers. If $f : D \to F$ is any function over some open subset $D \subseteq E$ and $x \in D$ is a point therein, then f is said to be *differentiable* in x, iff there is some linear map $L : E \to F$ such that

$$\lim_{h \to 0} \frac{\|f(x+h) - L(h) - f(x)\|_F}{\|h\|_E} \;=\; 0$$

Thereby (due to the triangle inequality) the map L is uniquely determined and called the *derivative* of f in x, written as: $df(x) := L$. If now $\mathcal{D}(x, F)$ denotes the set of all functions $f : D \to F$ that are differentiable in x, then we find that $\mathcal{D}(x, F)$ is a subspace of $\mathcal{F}(D, F)$ and that the derivation $f \mapsto df(x)$ is an $\mathbb{F}$-linear map as well:

$$\mathcal{D}(x, F) \to \mathcal{L}(E, F) \;:\; f \mapsto df(x)$$

Completion of Metric Spaces

(6.42) Definition:
Let (X, d) be a metric space, then a sequence $(x_n) \subseteq X$ is said to be a **Cauchy-sequence** if its elements come ever closer. Formally iff it satisfies the following property

$$\forall\, \varepsilon > 0\ \exists\, n(\varepsilon) \in \mathbb{N}\ \forall\, m, n \geq n(\varepsilon) \quad : \quad d\big(x_m, x_n\big) < \varepsilon$$

Let us denote the set of all these Cauchy-sequences by $\text{Cauchy}\,(X, d)$ and the set of all convergent series by $\text{Conv}\,(X, d)$. Recall that (x_n) is **convergent** iff there is some $x \in X$, such that

$$\forall\, \varepsilon > 0\ \exists\, n(\varepsilon) \in \mathbb{N}\ \forall\, n \geq n(\varepsilon) \quad : \quad d\big(x_n, x\big) < \varepsilon$$

In symbols we write $(x_n) \to x$ for this property. Generally any convergent sequence also is a Cauchy-sequence, that is we always have $\text{Conv}\,(X, d) \subseteq \text{Cauchy}\,(X, d)$. And we say that (X, d) is a **complete** metric space, iff the converse is true as well, that is iff we have

$$\text{Conv}\,(X, d) \;=\; \text{Cauchy}\,(X, d)$$

Prob We need to verify $\text{Conv}\,(X, d) \subseteq \text{Cauchy}\,(X, d)$: Suppose we have $(x_n) \to x$, then given any $\varepsilon > 0$ we can choose some $n(\varepsilon) \in \mathbb{N}$ such that for any $n \geq n(\varepsilon)$ we get $d(x_n, x) < \varepsilon/2$. Thus for m, $n \geq n(\varepsilon)$ we get $d(x_m, x_n) \leq d(x_m, x) + d(x, x_n) < \varepsilon/2 + \varepsilon/2 = \varepsilon$, which is just what we needed.

(6.43) Lemma: (viz. 1205)
Completion of metric spaces: Let (X, d) be a metric space and let $\text{Cauchy}\,(X, d)$ denote the set of

Cauchy-sequences on X. Then we obtain an equivalence relation on $\text{Cauchy}(X,d)$, by defining

$$(x_n) \sim (y_n) \quad :\Longleftrightarrow \quad \forall\, \varepsilon > 0\ \exists\, n(\varepsilon) \in \mathbb{N}\ \forall\, n \geq n(\varepsilon) \quad : \ d(x_n, y_n) \ < \ \varepsilon$$

The equivalence class of $(x_n) \in \text{Cauchy}(X,d)$ is written as $[x_n] := \{\, (y_n) \in \text{Cauchy}(X,d) \mid (x_n) \sim (y_n) \,\}$ and the quotient space of $\text{Cauchy}(X,d)$ under this relation is called the **completion** of (X,d)

$$\widehat{X} \ := \ \text{Cauchy}(X,d) \Big/ \sim$$

For any $x \in X$ the constant sequence $(x) \subseteq X$ is convergent and hence a Cauchy-sequence. This yields a canonical, injective map from X into its completion

$$\kappa : X \hookrightarrow \widehat{X} \ : \ x \mapsto [x]$$

Due to this construction all the sequences $(d(x_n, y_n)) \subseteq \mathbb{R}$ converge for any Cauchy-sequences (x_n), $(y_n) \in \text{Cauchy}(X,d)$. And thereby we also obtain a well-defined, metric $\widehat{d}$ on $\widehat{X}$ by letting

$$\widehat{d}\big([x_n],[y_n]\big) \ := \ \lim_{n\to\infty} d(x_n, y_n)$$

For any x, $y \in X$ we thereby get $\widehat{d}([x],[y]) = d(x,y)$ such that the canonical map $\kappa : X \hookrightarrow \widehat{X}$ also is continuous. And the image of κ is dense in $\widehat{X}$. That is: If we regard X as a subset of $\widehat{X}$ under this embedding, then its closure is the entire space $\widehat{X}$

$$\overline{\kappa(X)} \ = \ \widehat{X}$$

Most importantly: The completion $(\widehat{X}, \widehat{d})$ of (X,d) not only extends X canonically, but also is a complete metric space. That is every Cauchy-sequence of $(\widehat{X}, \widehat{d})$ already converges to some point in $\widehat{X}$.

required: $\mathbb{R}$ is hausdorff and complete required: $x_n \leq y_n \implies x \leq y$ and also if $x_n \leq a$ (for any $n \geq N$) then $x \leq a$ required: $(x_n \pm y_n) \to x \pm y$ and $(x_n \cdot y_n) \to xy$ and if we scratch $y_n = 0$ from (y_n) then also $(x_n / y_n) \to x/y$ metric groups and rings completion of metric groups and rings

6.4 Hilbert Spaces

inner product = special case of sesqui-linear form

6.5 Operatoralgebras

Chapter 7

Polynomial Rings

Polynomials are a powerful tool in algebra, as they simulate all the algebraic operations (finite additions, multiplications and powers) that are native to algebras. In this setting polynomials are the generic example of R-algebras and we will find some very powerful statements (like the lemma of Gauss or noetherian normalisation) of general importance by studying polynomials. On the other hand polynomial rings are very tame, as by definition the variables are independent of one and another. Therefore polynomials are the perfect stepping stone on the way to general algebras.

Also polynomials have been one of the origins of modern algebra. While the solution formula for quadratic equations is ancient, the formulas for cubic and quartic equations defied discovery until the 16. century by Cardano, resp. his student Ferrari and others. Interest grew (literally) as there was a lot of money to be made, by computing the best rates of interest for italian bankiers and traders. But mathematicians kept their insights a secret, at that time, for competetive reasons. So in fact these formulas were discovered independently by several mathematicians - apparently the time was just about right for these discoveries. Although the formulas for solving equations of degree 3 and 4 have been found in short sequel, equations of degree 5 remained unsolved. It took another 200 years until, the reason for this had been unearthed: In the 18. century Abel was able to prove, that there *is* no general formula to solve equations of degree 5 or higher - quite interesting, he had found general limits to what mathematics can do (much like Gödel's incompleteness theorem). This will be a major spin-off of Galois theory, which combines group theory with field extensions.

However we will not pursue the theory of solving polynomial equations right now, but rather chose a top-down approach: We start with the general concept of group rings $R[t \mid A]$ and only later specialize to $A = \mathbb{N}^n$ which yields the polynomial ring $R[t_1, \ldots, t_n]$ in n variables. And only after that we come full circle to study the special properties polynomial ring $R[t]$ in one variable. We will encounter group rings again, when we tackle representation theory.

For now we aim at the general theory: If we order the monomials in a reasonable way, we will be able to introduce Gröbner-bases (of ideals of polynomials) which provide powerful computational algorithms, such as Buchberger's algorithm, that determines whether a polynomial is contained in a certain ideal, or not. This is a powerful generalization of division with remainder of polynomials in one variable.

7.1 Monomial Orders

We have already introduced the polynomial ring $R[t]$ in one variable (over a commutative ring R) as an example in section 1.4. And we have also used this concept several times before (e.g. for the characteristic polynomial of a linear mapping). In this chapter we will now introduce a powerful generalization of this ring - the polynomial ring (also called group ring) $R[t \mid A]$. Thereby R is a commutative ring once more and A will be any commutative monoid. On the other hand polynomial rings are natural examples of graded algebras. So it may be advantageous to first study graded algebras as a general concept. This will be done in the subsequent section.
There are a multitude of special cases of this concept which we will regard in this chapter, as well. The most important special case will be the polynomial ring $R[t_1, \ldots, t_n]$ in (finitely many) variables. The polynomials $f \in R[t_1, \ldots, t_n]$ are the working horses of ring theory, as they describe all the compositions (addition, multiplication and powers) that can be performed in a ring. This makes the study of the polynomial ring a task of vast importance and likewise gives the theory its punch.
The polynomial ring $R[t]$ is included into this general theory as the polynomial ring $R[t \mid A]$ where A is chosen to be the the natural numbers $A = \mathbb{N}$. Yet the algabraic structure of $\mathbb{N}$ is not the sole important property for $R[t]$. The natural order $\leq$ on $\mathbb{N}$ is of no lesser importance. Therefore we will first study moniods A that carry an adequate order, as well.
So first recall the definition of a *linear order* (also called *total order*). If you are not familiar with this notion take a look at the introduction (section 0.3) or (re)read the beginning of section 2.1 for even more comments. So let us now introduce the basic concepts of ordered monoids:

(7.1) Definition:
Let $(A, +)$ be a commutative monoid and denote its neutral element by 0. Then we introduce the following notions: A is said to be **integral** iff for any α, β and $\gamma \in A$ we get the implication

$$\alpha + \gamma \;=\; \beta + \gamma \quad \Longrightarrow \quad \alpha \;=\; \beta$$

[in particular any commutative group A is an integral monoid]. Further A is said to be **solution-finite** iff for any fixed $\gamma \in A$ the equation $\alpha + \beta = \gamma$ has finitely many solutions only, formally that is

$$\forall\, \gamma \in A \;\; : \;\; \#\left\{\, (\alpha, \beta) \in A^2 \mid \alpha + \beta = \gamma \,\right\} \;<\; \infty$$

(7.2) Proposition: (viz. 1208)
If $(A, +)$ and $(B, +)$ are two commutative monoids, then their product $A \times B$ is another commutative monoid under the point-wise addition

$$(\alpha, \beta) + (\gamma, \delta) \;\; := \;\; (\alpha + \gamma,\, \beta + \delta)$$

The neutral element of $A \times B$ is $0 = (0_A, 0_B)$. And if both A and B are integral, resp. solution-finite then $A \times B$ is integral resp. solution finite again.

(7.3) Definition:

(i) The triple $(A, +, \leq)$ is said to be a **positively ordered monoid**, iff A is a commutative monoid under the addition $+$ and $\leq$ is a total, *positive* order on A. Formally we require the properties

(1) $(A, +)$ is a commutative monoid (with neutral element 0)

(2) $\leq$ is a linear order on A such that for any elements α, α' and $\beta \in A$ we get the implication

$$\alpha \leq \alpha' \quad \Longrightarrow \quad \alpha + \beta \leq \alpha' + \beta$$

(ii) The triple $(A, +, \leq)$ is said to be a **strictly positively ordered monoid**, iff A is commutative monoid under the addition $+$ and $\leq$ is a total, *strictly positive* order on A. Formally again we require

(1) $(A, +)$ is a commutative monoid (with neutral element 0)

(2) $\leq$ is a linear order on A such that for any elements α, α' and $\beta \in A$ we get the implication

$$\alpha < \alpha' \quad \Longrightarrow \quad \alpha + \beta < \alpha' + \beta$$

Nota that we used the notation $a < b \ :\Longleftrightarrow \ a \leq b$ and $a \neq b$ here. Also it is clear that a strictly positively ordered monoid already is a positively ordered monoid, as $\alpha = \alpha'$ implies $\alpha + \beta = \alpha' + \beta$ in any case.

(iii) Finally $(A, +, \leq)$ is said to be a **well-ordered monoid** and $\leq$ is said to be a **monomial well-ordering** on $(A, +)$ iff A is commutative monoid under the addition $+$ and $\leq$ is a *well-ordering* on A. Formally we require the following properties

(1) $(A, +, \leq)$ is a positively ordered monoid (with neutral element 0)

(2) $\leq$ is a *well-ordering* on A, that is a total order, such that any non-empty subset M of A has a minimal element. Formally the latter can be written as

$$\forall \emptyset \neq M \subseteq A \ \exists \mu_* \in M \quad \text{such that} \quad \forall \mu \in M \text{ we get } \mu_* \leq \mu$$

(7.4) Remark:
If now $(A, +, \leq)$ is a positively ordered monoid, we extend A to $\overline{A}$ by formally picking up a new element (that we introduce a new symbol $-\infty$ to A) $\overline{A} := A \cup \{ -\infty \}$. We then extend the composition $+$ and the order $\leq$ of A to $\overline{A}$ by defining the following operations and relations for any $\alpha \in A$

$$\begin{aligned} (-\infty) &\neq \alpha \\ (-\infty) &\leq \alpha \\ (-\infty) + \alpha &:= -\infty \\ \alpha + (-\infty) &:= -\infty \end{aligned}$$

Nota clearly $(\overline{A}, +)$ is a commutative monoid again and if $\leq$ has been a positive order or even a monomial well-ordering on A then the extended order on $\overline{A}$ is a positive order resp. a monomial well-ordering again.

(7.5) Example:
The standard example of a monoid that we will use later is $\mathbb{N}^n$ under the point-wise addition as the composition. However we will already discuss a slight generalization of this monoid here. Let $I \neq \emptyset$ be any non-empty index set and let us define the set

$$\mathbb{N}^{\oplus I} \quad := \quad \Big\{ \alpha \in \mathbb{N}^I \mid \#\{ i \in I \mid \alpha_i \neq 0 \} < \infty \Big\}$$

If I is finite, say $I = 1 \dots n$, then it is clear, that $\mathbb{N}^{\oplus(1\dots n)} = \mathbb{N}^n$. We now turn this set into a commutative monoid by defining the composition $+$ to be the point-wise addition, i.e. for any $\alpha = (\alpha_i)$ and $\beta = (\beta_i)$

$$(\alpha_i) + (\beta_i) \quad := \quad (\alpha_i + \beta_i)$$

And it is clear that this composition turns $\mathbb{N}^{\oplus I}$ into a commutative monoid, that is integral and solution-finite (for any $\gamma \in \mathbb{N}^{\oplus I}$ the set of solutions (α, β) of $\alpha + \beta = \gamma$ is given to be $\{ (\alpha, \gamma - \alpha) \mid \alpha_i \leq \gamma_i \}$, which is finite, as $\gamma_i = 0$ for all but finitely many $i \in I$). For any $i \in I$ we now define

$$\delta_i \ : \ I \to \mathbb{N} \ : \ j \mapsto \delta_{i,j}$$

where $\delta_{i,j}$ denotes the Kronecker symbol (e.g. refer to the notation and symbol list). From the construction it is clear, that any $\alpha = (\alpha_i) \in \mathbb{N}^{\oplus I}$ is a (uniquely determined) *finite* sum of these δ_i since

$$(\alpha_i) \quad = \quad \sum_{i \in I} \alpha_i \, \delta_i$$

This sum in truth is finite as only finitely many coefficients α_i are non-zero and we can omit those $i \in I$ with $\alpha_i = 0$ from the sum. This enables us to introduce some notation here that will be put to good use:

- Let us first define the **absolute value** of $\alpha = (\alpha_i) \in \mathbb{N}^{\oplus I}$ to be the sum of its entries [this is the 1-norm of α] and the **norm** of α to be the maximum entry of α [this is the ∞-norm of α]:

$$\begin{aligned} |\alpha| \quad &:= \quad \sum_{i \in I} \alpha_i \\ \|\alpha\| \quad &:= \quad \max\{ \alpha_i \mid i \in I \} \end{aligned}$$

- For a fixed weight $\omega \in \mathbb{N}^I$ we introduce the **weighted sum** of α (note that this is well-defined, as $\alpha \in \mathbb{N}^{\oplus I}$ only has finitely many non-zero entries and hence the sum is finite only)

$$|\alpha|_\omega \quad := \quad \sum_{i \in I} \omega_i \, \alpha_i$$

- Another often useful notation (for any $\alpha \in \mathbb{N}^{\oplus I}$ and any $k \in \mathbb{N}$ with $\|\alpha\| \leq k$) are the **faculty** and **binomial coefficients**, which are defined to be

$$\begin{aligned} \alpha! \quad &:= \quad \prod_{i \in I} \alpha_i! \\ \binom{k}{\alpha} \quad &:= \quad \prod_{i \in I} \binom{k}{\alpha_i} \end{aligned}$$

- And if $x = (x_i) \in R^I$ is an I-tupel of elements of a commutative ring $(R, +, \cdot)$ we finally introduce the notations (note that these are well-defined again, as $\alpha \in \mathbb{N}^{\oplus I}$ has only finitely many $\alpha_i \neq 0$)

$$\begin{aligned} \alpha x &:= \sum_{i \in I} \alpha_i \, x_i \\ x^\alpha &:= \prod_{i \in I} x_i^{\alpha_i} \end{aligned}$$

(7.6) Proposition: (viz. 1208)

(i) Let A be any set and $\leq \subseteq A \times A$ be a linear order on A. Then any finite, non-empty subset $M \subseteq A$ has uniquely determined minimal and a maximal elements. I.e. for any $M \subseteq A$ with $1 \leq \#M < \infty$ we get

$$\begin{aligned} \exists!\, \mu_* \in M \,:\, \forall\, \mu \in M \;&:\; \mu_* \leq \mu \\ \exists!\, \mu^* \in M \,:\, \forall\, \mu \in M \;&:\; \mu \leq \mu^* \end{aligned}$$

Nota we will refer to these uniquely determined minimal and maximal elements of M by writing $\min(M) := \mu_*$ and $\max(M) := \mu^*$ respectively.

(ii) Let A be any set and $\leq \subseteq A \times A$ be a well-ordering on A. Then any non-empty subset $M \subseteq A$ has a uniquely determined minimal element. I.e. for any $M \subseteq A$ with $M \neq \emptyset$ we get

$$\exists!\, \mu_* \in M \,:\, \forall\, \mu \in M : \mu_* \leq \mu$$

(iii) Let $(A, +)$ be a commutative monoid and let $\leq \subseteq A \times A$ be a linear order on A. Then the following three statements are equivalent

(a) A is integral and $\leq$ is a positive order on A

(b) $(A, +, \leq)$ is a strictly positively ordered monoid

(c) for any $\alpha, \beta, \gamma \in A$ we get $\alpha < \beta \iff \alpha + \gamma < \beta + \gamma$

(iv) Let $(A, +, \leq)$ be a strictly positively ordered monoid. Let further M, $N \subseteq A$ be any two subsets and $\mu_* \in M$ respectively $\nu_* \in N$ be minimal elements of M and N, that is we have

$$\forall\, \mu \in M \,:\, \mu_* \leq \mu \quad \text{and} \quad \forall\, \nu \in N \,:\, \nu_* \leq \nu$$

Then for any elements $\mu \in M$ and $\nu \in N$ we get: If $\mu + \nu$ equals the sum $\mu_* + \nu_*$ of minimal elements then necessarily $\mu = \mu_*$ and $\nu = \nu_*$ are these minimal elements already, formally

$$\mu + \nu \,=\, \mu_* + \nu_* \quad \Longrightarrow \quad \mu \,=\, \mu_* \;\text{ and }\; \nu \,=\, \nu_*$$

Nota the same is true for maximal elements $\mu^* \in M$ and $\nu^* \in N$. That is if $\mu \leq \mu^*$ and $\nu \leq \nu^*$ for any $\mu \in M$ and $\nu \in N$ respectively, then $\mu + \nu = \mu^* + \nu^*$ implies $\mu = \mu^*$ and $\nu = \nu^*$, as well.

(vii) If $(A, +, \leq)$ is a (strictly) positively ordered monoid, then we define the *inverse order* $\geq$ by letting: $\alpha \geq \beta \;:\Longleftrightarrow\; \beta \leq \alpha$. And thereby $(A, +, \geq)$ is a (strictly) positively ordered monoid, again.

(viii) If $(A,+,\leq)$ is an integral, positively ordered monoid such that for any $\gamma \in A$ the set $\{\, \alpha \in A \mid \alpha \leq \gamma \,\}$ is finite, then A is solution-finite, as well.

(ix) If $(A,+,\leq)$ is an integral, positively ordered monoid, that also is solution-finite, then $(0,0)$ is the one and only solution for $\alpha+\beta=0$. That is for any α, $\beta \in A$ we get the implication

$$\alpha+\beta \;=\; 0 \quad\Longrightarrow\quad \alpha \;=\; 0 \;=\; \beta$$

(7.7) Example: (viz. 1210)
Let now $(I,\leq)$ be a well-ordered set (i.e. $I \neq \emptyset$ is a non-empty set and $\leq$ is a well-ordering on I) and fix any weight $\omega \in \mathbb{N}^I$. Then we introduce two different linear orders on the commutative monoid $(\mathbb{N}^{\oplus I},+)$. Of these the ω-graded lexicographic order will be the standard order we will employ in later sections. Thus consider $\alpha=(\alpha_i)$ and $\beta=(\beta_i) \in \mathbb{N}^{\oplus I}$ and define

- **Lexicographic Order**

$$\alpha \leq_{\text{lex}} \beta \quad :\Longleftrightarrow \quad (\alpha=\beta) \text{ or } (*)$$

$$(*) \;:=\; \exists k \in I \text{ such that } \alpha_k < \beta_k \text{ and } \forall\, i<k \,:\, \alpha_i=\beta_i$$

 Then the lexicographic order $\leq_{\text{lex}}$ is strictly positive, i.e. the triple $(\mathbb{N}^{\oplus I},+,\leq_{\text{lex}})$ is a strictly positively ordered monoid. And in case of $I=1\ldots n$ is finite, we will see that $\leq_{\text{lex}}$ even is a well-ordering, i.e. the triple $(\mathbb{N}^n,+,\leq_{\text{lex}})$ is a well-ordered monoid, too.

- **ω-Graded Lexicographic Order**

$$\alpha \leq_\omega \beta \quad :\Longleftrightarrow \quad (|\alpha|_\omega < |\beta|_\omega) \text{ or } (|\alpha|_\omega = |\beta|_\omega \text{ and } \alpha \leq_{\text{lex}} \beta)$$

 Analogously the ω-graded lexicographic order $\leq_\omega$ is strictly positive, i.e. $(\mathbb{N}^{\oplus I},+,\leq_\omega)$ is a strictly positively ordered monoid. And in the case $I=1\ldots n$ is finite it even is a well-ordering, i.e. the triple $(\mathbb{N}^n,+,\leq_\omega)$ is a well-ordered monoid once more.

(7.8) Remark:
For an arbitrary, non-empty set $I \neq \emptyset$ the *well-ordering theorem* says, that there *is* some linear well-ordering $\leq$ on I. Even though we can't put it explicitly, there is some. However the theorem does not not guarantee that this ordering is compatible with addition, i.e. whether A will be turned into a positively ordered monoid. However this is not what we aim for:
We already know, that $(\mathbb{N}^{\oplus I},+)$ is a commutative, integral monoid. Now the example above also tells us that$(\mathbb{N}^{\oplus I},+,\leq_{\text{lex}})$ even is a strictly positively ordered monoid. And if I is finite, then we even have the well-ordering property. The lexicographic order is nice to have, since $\mathbb{N}^n$ will be the standard monoid for polynomial rings. We will not pursue the general theory any further, as this suffices for Gröbner-bases.

(7.9) Remark: (■)
We wish to append two further linear orders on $(\mathbb{N}^{\oplus I}, +)$. However we will not require these any further and hence abstain from proving any details about them. The interested reader is asked to refer to [Cox, Little, O'Shaea; Using Algebraic Geometry, GTM 185] for more comments on these.

- **Reverse Graded Lexicographic Order**

$$\alpha \leq_{\text{rgl}} \beta \quad :\Longleftrightarrow \quad (\alpha = \beta) \text{ or } (|\alpha| < |\beta|) \text{ or } (|\alpha| = |\beta| \text{ and } (2))$$

$$(2) \quad := \quad \exists k \in I \text{ such that } \alpha_k > \beta_k \text{ and } \forall i < k \,:\, \alpha_i = \beta_i$$

 Just like $\leq_\omega$ the reverse graded lexicographic order $\leq_{\text{rgl}}$ is positive and in the case of $I = 1 \dots n$ it even is a well-ordering again.

- **Bayer-Stillman Order**
 For the fourth order we will require $I = 1 \dots n$ already. Then we fix any $m \in 1 \dots n$ and obtain another monomial well-ordering on $\mathbb{N}^n$

$$\alpha \leq_{\text{bs}(m)} \beta \quad :\Longleftrightarrow \quad (3) \text{ or } ((4) \text{ and } \alpha \leq_{\text{rgl}} \beta)$$

$$(3) \quad := \quad \alpha_1 + \dots + \alpha_m < \beta_1 + \dots + \beta_m$$

$$(4) \quad := \quad \alpha_1 + \dots + \alpha_m = \beta_1 + \dots + \beta_m$$

7.2 Defining Polynomials

Polynomials are of tremendous importance in ring-theory, since they embody all the operations of rings and fields. We already introduced the polynomial ring in one variable as an example, but now we wish to turn to the general setting. In this section we only require the notions of section 7.1 and not the graded algebras of section 7.4 yet. Later on, in section 7.3 we will specify this general setting to the cases that are used most often, the polynomial rings $R[t_1, \ldots, t_n]$ at their center.

(7.10) Definition:
Let $(R, +, \cdot)$ be a commutative ring (denoting its neutral elements by 0 and 1 as usual) and let $(A, +)$ be a monoid (denoting its neutral element by 0, too), then we introduce the following notions

(i) We define the set of **formal A-series** over R to be all the functions from A to R and denote it by

$$R[\![t \mid A]\!] \;:=\; \{\, f \mid f : A \to R : \alpha \mapsto f[\alpha] \,\}$$

Note that in order to get an unambiguous notation we have already abandoned our standard notation and wrote $f[\alpha] := f(\alpha) \in R$ instead. Also please be aware that the use of the variable symbol t in $R[\![t \mid A]\!]$ is purely notational and will be explained in the subsequent remark.

We now turn $R[\![t \mid A]\!]$ into an R-module by defining the following addition and scalar-multiplication

$$f + g \;:\; A \to R \;:\; \alpha \mapsto f[\alpha] + g[\alpha]$$

$$a f \;:\; A \to R \;:\; \alpha \mapsto a \cdot f[\alpha]$$

If A is solution-finite the formal A-series $R[\![t \mid A]\!]$ even becomes an R-algebra under the following multiplication - where $f, g \in R[\![t \mid A]\!]$ and $a \in R$ of course and $\sum_{\alpha+\beta=\gamma}$ denotes the (finite) sum over the set $\{\, (\alpha, \beta) \in A^2 \mid \alpha + \beta = \gamma \,\}$ of all pairs (α, β) that satisfy $\alpha + \beta = \gamma$

$$f \cdot g \;:\; A \to R \;:\; \gamma \mapsto \sum_{\alpha+\beta=\gamma} f[\alpha] \cdot g[\beta]$$

(ii) We define the set of **A-polynomials** over R to be the functions from A to R that are non-zero on finitely many elements $\alpha \in A$ only

$$R[t \mid A] \quad:=\quad \{\, f : A \to R \mid \;\; \#\{\, \alpha \in A \mid f[\alpha] \neq 0 \,\} < \infty \,\}$$

Nota it is clear that the polynomials $R[t \mid A]$ thereby become an R-sub-module of the formal A-series $R[\![t \mid A]\!]$. And $R[t \mid A]$ even is an R-algebra under the above multiplication, even if A is not solution-finite, as the products $f[\alpha] \cdot g[\beta]$ are zero for all but finitely many $(\alpha, \beta) \in A^2$, such that the sum $\sum_{\alpha+\beta=\gamma}$ remains finite, even if $\{\, \alpha + \beta = \gamma \,\}$ is infinite.

(7.11) Remark:

(i) From the definition of the polynomial ring $R[t \mid A]$ is clear, that this is a free R-module of rank $|A|$ as an R-basis of $R[t \mid A]$ is given by $\{ t^\alpha \mid \alpha \in A \}$, where the **monomial** t^α is defined to be the following A-polynomial

$$t^\alpha \;:\; A \to R \;:\; \beta \mapsto \begin{cases} 0 & \text{for } \alpha \neq \beta \\ 1 & \text{for } \alpha = \beta \end{cases}$$

And thereby the monomials satisfy the following important multiplicative property for any $\alpha, \beta \in A$

$$t^\alpha \, t^\beta \quad = \quad t^{\alpha+\beta}$$

Prob consider any $\gamma \in A$, then $(t^\alpha \, t^\beta)[\gamma] = \sum_{\alpha'+\beta'=\gamma} \delta_{\alpha',\alpha}\delta_{\beta',\beta}$ and the product $\delta_{\alpha',\alpha}\delta_{\beta',\beta}$ yields 1 if and only if $\alpha' = \alpha$ and $\beta' = \beta$. Hence if $\gamma = \alpha + \beta$ then we get $(t^\alpha \, t^\beta)[\gamma] = 1$ for this one combination. And if $\gamma \neq \alpha + \beta$ then the combination $\alpha' = \alpha$ and $\beta' = \beta$ does not occur, such that $(t^\alpha \, t^\beta)[\gamma] = 0$. But this is precisely, what $t^{\alpha+\beta}$ does and hence $t^\alpha \, t^\beta = t^{\alpha+\beta}$ as claimed.

(ii) We will use this standard basis most often and the variable symbol t in $R[t \mid A]$ denotes just what symbols t^α we will use for the monomials. Now any polynomial $f \in R[t \mid A]$ has a unique representation in this standard basis, given by

$$f \quad = \quad \sum_{\alpha \in A} f[\alpha] \, t^\alpha$$

Note that this sum in truth is finite only, as (by construction) the coefficients $f[\alpha]$ are zero for all but finitely many $\alpha \in A$.

(iii) We will formally adopt this representation to $R[\![t \mid A]\!]$. Note however that this sum *can be* infinite and hence may well have absolutely no meaning apart from fixing the coefficients $f[\alpha]$ of the power series f. That is, we also write

$$\sum_{\alpha \in A} f[\alpha] \, t^\alpha \quad := \quad (A \to R \;:\; \alpha \mapsto f[\alpha])$$

(iv) This is precisely the reason why we defined the multiplication of formal power series and polynomials, in the way we did: This multiplication neatly incorporates the general rule distributivity. Combined with the notation in (iii) the multiplication of formal power series (if A is solution-finite) and polynomials (in general) f and g yields

$$\left(\sum_{\alpha \in A} f[\alpha] t^\alpha \right) \cdot \left(\sum_{\beta \in A} g[\beta] t^\beta \right) \quad = \quad \sum_{\gamma \in A} \left(\sum_{\alpha+\beta=\gamma} f[\alpha] \, g[\beta] \right) t^\gamma$$

(7.12) Proposition: (viz. 791)
Let $(R,+,\cdot)$ be a commutative ring and $(A,+)$ be a monoid, then all of the following statements are true

(i) The unit element $\mathbf{1}$ of the polynomial ring $R[t \mid A]$ is given by

$$\mathbf{1} \;=\; t^0 \;:\; A \to R \;:\; \alpha \mapsto \begin{cases} 1 & \text{if} \quad \alpha = 0 \\ 0 & \text{if} \quad \alpha \neq 0 \end{cases}$$

(ii) R is embedded into all the polynomial rings over R. That is: We have an injective homomorphism of R-algebras by virtue of

$$\iota \;:\; R \hookrightarrow R[t \mid A] \;:\; a \mapsto a\,\mathbf{1}$$

In this sense R will always be interpreted as a sub-ring of $R[t \mid A]$, e.g. if $f \in R[t \mid A]$ is a polynomial we will write $f \in R$ to express that f is of the form $f = a\,\mathbf{1}$ for some R$a \in R$ and such a polynomial will be called a **constant** polynomial over R.

(iii) If $(B,+)$ is a commutative monoid, such that $A \leq_o B$ is a submonoid of B, then we find a canonical embedding of the polynomial rings

$$R[t \mid A] \hookrightarrow R[t \mid B] \;:\; f \mapsto \left(\beta \mapsto \begin{cases} f[\beta] & \text{if} \quad \beta \in A \\ 0 & \text{if} \quad \beta \notin A \end{cases}\right)$$

I.e. this map is a monomorphism of R-algebras. And if B is solution-finite then this embedding extends to the rings of formal power series

$$R[\![t \mid A]\!] \hookrightarrow R[\![t \mid B]\!] \;:\; f \mapsto \left(\beta \mapsto \begin{cases} f[\beta] & \text{if} \quad \beta \in A \\ 0 & \text{if} \quad \beta \notin A \end{cases}\right)$$

(iv) If $(S,+,\cdot)$ is another commutative ring and $\varphi : R \to S$ is a homomorphism of rings, then we obtain another homomorphism $\overline{\varphi}$ of R-modules

$$\overline{\varphi} \;:\; R[\![s \mid A]\!] \;\to\; S[\![t \mid A]\!] \;:\; \sum_{\alpha \in A} f[\alpha]\, t^\alpha \;\mapsto\; \sum_{\alpha \in A} \varphi(f[\alpha])\, t^\alpha$$

Clearly this homomorphism restricts to the polynomial ring and in fact it is a homomorphism of R-algebras there. Also $\overline{\varphi}$ is a homomorphism of R-algebras, in case A is solution-finite

$$\overline{\varphi} \;:\; R[s \mid A] \;\to\; S[t \mid A] \;:\; \sum_{\alpha \in A} f[\alpha]\, t^\alpha \;\mapsto\; \sum_{\alpha \in A} \varphi(f[\alpha])\, t^\alpha$$

Let us abbreviate any one of the words *injective*, *surjective* or *bijective* by $\star$, then we obtain the following property: If φ is $\star$, then $\overline{\varphi}$ is $\star$, as well.

(v) The polynomial ring $R[t \mid A]$ is commutative iff the monoid A is such. And if A is solution-finite the same is true for the formal A-series. That is we have the following two equivalences

$$\begin{aligned} R[t \mid A] \text{ is commutative} \quad &\Longleftrightarrow \quad A \text{ is commutative} \\ R[\![t \mid A]\!] \text{ is commutative} \quad &\Longleftrightarrow \quad A \text{ is commutative} \end{aligned}$$

(vi) Consider any two commutative monoids $(A,+)$ and $(B,+)$. Then the polynomial ring over B over the polynomial ring over A is isomorphic to the polynomial ring over $A \times B$. That is we have the isomorphy (of R-algebras)

$$\begin{array}{rcl} R[s \mid A][t \mid B] & \xrightarrow{\sim} & R[x \mid A \times B] \\ \displaystyle\sum_{\beta\in B}\left(\sum_{\alpha\in A} f[\beta][\alpha]\, s^{\alpha}\right) t^{\beta} & \mapsto & \displaystyle\sum_{(\alpha,\beta)\in A\times B} f[\beta][\alpha]\, x^{(\alpha,\beta)} \end{array}$$

And if both A and B are solution-finite, then the same isomorphism runs between the formal power series over B over A and over $A \times B$. Formally again

$$\begin{array}{rcl} R[\![s \mid A]\!][\![t \mid B]\!] & \xrightarrow{\sim} & R[\![x \mid A \times B]\!] \\ \displaystyle\sum_{\beta\in B}\left(\sum_{\alpha\in A} f[\beta][\alpha]\, s^{\alpha}\right) t^{\beta} & \mapsto & \displaystyle\sum_{(\alpha,\beta)\in A\times B} f[\beta][\alpha]\, x^{(\alpha,\beta)} \end{array}$$

(vii) Let $(A,+,\leq)$ be a positively ordered monoid such that $(A,+)$ even is integral and let $\star$ abbreviate one of the words *integral domain* or *reduced ring*. Then the following two statements are equivalent

(a) R is a $\star$

(b) $R[t \mid A]$ is a $\star$

And if R and hence $R[t \mid A]$ is an integral domain, we denote its quotient field by $R(t \mid A)$, which is called the field of *rational fractions* of R over A. Formally that is

$$R(t \mid A) \;:=\; \mathrm{QUOT}\big(R[t \mid A]\big)$$

(viii) Let $(A,+,\leq)$ be an positively ordered monoid such that $(A,+)$ even is integral and for any $\gamma \in A$ the set $\{\, \alpha \in A \mid \alpha \leq \gamma \,\}$ is finite. Again let $\star$ abbreviate one of the words *integral domain* or *reduced ring*. Then we also have the equivalence, of the following two statements

(a) R is a $\star$

(b) $R[\![t \mid A]\!]$ is a $\star$

And if R and hence $R[\![t \mid A]\!]$ is an integral domain, we denote its quotient field (which does have a special name, of its own) by

$$R((t \mid A)) \;:=\; \mathrm{QUOT}\big(R[\![t \mid A]\!]\big)$$

(7.13) Example:
Let $(R,+,\cdot)$ be a commutative ring, $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ an ideal of R and let $(A,+)$ be a monoid. We consider the residue ring $S := R/\mathfrak{a}$ and the canonical epimorphism $\varrho : R \to S : b \mapsto b + \mathfrak{a}$. Then the induced homomorphism $\overline{\varrho} : R[t \mid A] \to S[t \mid A]$ is surjective and has the kernel $\mathrm{kn}(\overline{\varrho}) = \mathfrak{a}[t \mid A]$ which is to say $\mathfrak{a}[t \mid A] := \{\, f \in R[t \mid A] \mid \forall\, \alpha \in A : f[\alpha] \in \mathfrak{a} \,\}$. In particular we obtain an isomorphy of R-algebras

$$R[t \mid A] \Big/ \mathfrak{a}[t \mid A] \;\xrightarrow{\sim}\; \Big(R \Big/ \mathfrak{a}\Big)\,[t \mid A] \;:\; f + \mathfrak{a}[t \mid A] \mapsto \sum_{\alpha\in A} \big(f[\alpha] + \mathfrak{a}\big)\, t^{\alpha}$$

Prob by (7.12.(iv)) $\overline{\varrho}$ is an epimorphism, too and $\overline{\varrho}(f) = 0$ is equivalent to $f[\alpha] \in \mathfrak{a}$ for any $\alpha \in A$. In other words this is $f \in \mathfrak{a}[t \mid A]$, so the isomorphy is granted by the first isomorphism theorem.

(7.14) Lemma: (viz. 794)
Let now $(R, +, \cdot)$ and $(S, +, \cdot)$ be commutative rings and $(A, +)$ be a commutative monoid. Further suppose that $\varphi : R \to S$ is a homomorphism of rings and $\sigma : A \to S$ is a homomorphism of monoids from $(A, +)$ to $(S, \cdot)$ (see the remark below, for the explicit properties, we require of σ)

$$\begin{aligned} \varphi &: R \to S \quad \text{is a ring-homomorphism and} \\ \sigma &: A \to S \quad \text{is a monoid-homomorphism} \end{aligned}$$

Together φ and σ induce a ring-homomorphism $\sigma_\varphi : R[t \mid A] \to S$ that also satifies $\sigma_\varphi(af) = \varphi(a) \cdot \sigma_\varphi(f)$ for any $a \in R$ and $f \in R[t \mid A]$. And this homomorphism is uniquely determined by the properties

- $\forall\ \lambda \in R$ we get $\sigma_\varphi(\lambda \mathbf{1}) = \varphi(\lambda)$
- $\forall\ \alpha \in A$ we get $\sigma_\varphi(t^\alpha) = \sigma(\alpha)$

(7.15) Remark:

- By the property that σ is a monoid-homomorphism we understand that $\sigma(0_A) = 1_S$ and that for any $\alpha, \beta \in A$ we get $\sigma(\alpha + \beta) = \sigma(\alpha) \cdot \sigma(\beta)$.
- Note that this ring-homomorphism σ_φ can be given explicitly: It simply is the R-linear expansion by $a \mapsto \varphi(a)$ of $t^\alpha \mapsto \sigma(\alpha)$, that is σ_φ is given to be

$$\sigma_\varphi\left(\sum_{\alpha \in A} a_\alpha\, t^\alpha\right) \quad = \quad \sum_{\alpha \in A} \varphi(a_\alpha)\, \sigma(\alpha)$$

- The standard situation is $A = \mathbb{N}^{\oplus I}$ and S an R-algebra of course. In this case we usually fix any I-tuple of elements $x = (x_i) \in R^I$ and take $\varphi : a \mapsto a1_S$ to be the *structural homomorphism* and σ to be the map $\sigma : \alpha \mapsto x^\alpha := \prod_i x_i^{\alpha(i)}$. Note that this product is well-defined, as $\alpha(i) = 0$ for all but finitely many $i \in I$. Refer to (7.52) for more comments on this. Then we get

$$f(x) \quad := \quad \sigma_{\mathbb{1}}(f) \quad = \quad \sum_{\alpha \in \mathbb{N}^{\oplus I}} f[\alpha]\, x^\alpha$$

(7.16) Remark: (viz. 795)
This proposition has an strange consequence: *Any* commutative ring $(R, +, \cdot)$ is the epimorphic image of an integral domain. That is there is an integral domain $(S, +, \cdot)$ and a surjective homomorphism ϱ of rings of the form

$$\varrho \ : \ S \ \twoheadrightarrow \ R$$

(7.17) Definition:
Let $(R,+,\cdot)$ be a commutative ring and $(A,+)$ be a commutative monoid. Further fix a total order $\leq$ on A then we define the following notions

(i) For a polynomial $f \in R[t \mid A]$ we define the **degree** $\deg(f) \in A \cup \{-\infty\}$ of f to be the maximal index $\alpha \in A$ such that $f[\alpha] \neq 0$. If there is none (i.e. $f = 0$), then we let $\deg(f) = -\infty$. Altogether

$$\deg(f) := \begin{cases} \max\{\alpha \in A \mid f[\alpha] \neq 0\} \text{ if } f \neq 0 \\ -\infty \text{ if } f = 0 \end{cases}$$

(ii) And thereby we define the **leading coefficient** $\operatorname{lc}(f) \in R$ of $f \in R[t \mid A]$ to be this non-zero coefficient $f[\alpha] \in R \setminus \{0\}$ of f, for which $\alpha = \deg(f)$ is maximal. If $f = 0$, we let $\operatorname{lc}(f) := 0 \in R$ instead. If $\operatorname{lc}(f) = 1 \in R$, then f is said to be **monic**. Altogether

$$\operatorname{lc}(f) := \begin{cases} f[\deg(f)] \text{ if } f \neq 0 \\ 0 \text{ if } f = 0 \end{cases}$$

(iii) Further we define the **leading monomial** $\operatorname{lm}(f) \in R[t \mid A]$ of $f \in R[t \mid A]$ to be this monomial t^α for which $\alpha = \deg(f)$ is maximal. If $f = 0$, we let $\operatorname{lm}(f) := 0 \in R[t \mid A]$ instead. Altogether

$$\operatorname{lm}(f) := \begin{cases} t^{\deg(f)} \text{ if } f \neq 0 \\ 0 \text{ if } f = 0 \end{cases}$$

(iii) Finally we introduce the **leading term** $\operatorname{lt}(f) \in R[t \mid A]$ of $f \in R[t \mid A]$ to be $f[\alpha]\, t^\alpha$ for this maximal $\alpha = \deg(f)$ again. If $f = 0$, we let $\operatorname{lt}(f) := 0 \in R[t \mid A]$, as before. Therefore we can either take $\operatorname{lt}(f) = \operatorname{lc}(f) \operatorname{lt}(f)$ or explicitly define $\operatorname{lt}(f)$ to be

$$\operatorname{lt}(f) := \begin{cases} f[\deg(f)]\, t^{\deg(f)} \text{ if } f \neq 0 \\ 0 \text{ if } f = 0 \end{cases}$$

Note if we are dealing with several total orders e.g. $\leq_1$ and $\leq_2$ then we will use subscripts such as $\deg_1$ or $\operatorname{lc}_2, \ldots$ to denote which of these orders we refer to.

(7.18) Proposition: (viz. 812)
Let $(R,+,\cdot)$ be any commutative ring, $(A,+)$ be a commutative monoid equipped with a positive order $\leq$ and let $f, g \in R[t \mid A]$ be two polynomials. Then the following (in)equalities hold true

$$\begin{aligned} \deg(f+g) &\leq \max\{\deg(f), \deg(g)\} \\ \deg(f \cdot g) &\leq \deg(f) + \deg(g) \\ \operatorname{lt}(f) &= \operatorname{lc}(f) \cdot \operatorname{lm}(f) \end{aligned}$$

If R is an integral domain and A is integral, too then the leading coefficient of the product $f \cdot g$ is the product of the leading terms of f and g and hence we obtain some further, noteworthy equalities

$$\begin{aligned} \deg(f \cdot g) &= \deg(f) + \deg(g) \\ \operatorname{lc}(f \cdot g) &= \operatorname{lc}(f) \cdot \operatorname{lc}(g) \\ \operatorname{lm}(f \cdot g) &= \operatorname{lm}(f) \cdot \operatorname{lm}(g) \\ \operatorname{lt}(f \cdot g) &= \operatorname{lt}(f) \cdot \operatorname{lt}(g) \end{aligned}$$

Nota even if R is any commutative ring (not necessarily an integral domain) and A is integral, then the four equalities above hold true, if at least on of the polynomials f or g is monic.

(7.19) Remark:
In the proof of (7.18) we even saw a little more: If R is an arbitrary commutative ring (not necessarily an integral domain) we obtain the equality for the degree in most cases, namely if the leading coefficients do not cancel each other. That is if $f, g \in R[t \mid A]$ are two polynomials, then we still get the implications

$$\begin{aligned} \operatorname{lc}(f) + \operatorname{lc}(g) \neq 0 \quad &\Longrightarrow \quad \deg(f+g) \;=\; \max\{\, \deg(f), \deg(g) \,\} \\ \operatorname{lc}(f) \cdot \operatorname{lc}(g) \neq 0 \quad &\Longrightarrow \quad \deg(f \cdot g) \;=\; \deg(f) + \deg(g) \end{aligned}$$

However these implications are not very useful, as for general polynomials we just don't know anything about their leading coefficients. Yet for a monic f and non-zero $g \in R[t]$ we have $\operatorname{lc}(f) \cdot \operatorname{lc}(g) = \operatorname{lc}(g) \neq 0$ and hence $\deg(f \cdot g) = \deg(f) + \deg(g)$. Easy counterexamples, where the degree truly decreases, are easy to provide - e.g. consider the base ring $R := \mathbb{F}_6$ then

$$\begin{aligned} (t+1) + (-t+1) &= 2 \\ (2t+1) \cdot (3t-1) &= t-1 \end{aligned}$$

7.3 The Standard Cases

In the previous section we have introduced the notion of a polynomial ring $R[t \mid A]$ over an arbitrary commutative monoid A. We also studied ordered monoids at the beginning of this chapter. The most important case however is the monoid $\mathbb{N}^{\oplus I}$ which has been introduced in example (7.5). This monoid is commutative, integral and solution finite and e.g. the graded lexicographic order is a positive well-ordering on it. This monoid will give rise to the polynomial ring $R[t_i \mid i \in I]$ which can be seen as the base ring R to which I-many algebraically independent elements t_i have been added. In complete analogy to the construction of $\mathbb{N}^{\oplus I}$ we will regard the monoid (in fact even a free group) $\mathbb{Z}^{\oplus I}$

$$\mathbb{Z}^{\oplus I} \quad := \quad \left\{ \alpha \in \mathbb{Z}^I \mid \#\{ i \in I \mid \alpha_i \neq 0 \} < \infty \right\}$$

If I is finite, say $I = 1 \dots n$, then it is clear, that $\mathbb{Z}^{\oplus(1\dots n)} = \mathbb{Z}^n$. We now turn this set into a commutative group by taking to the same point-wise addition as on $\mathbb{N}^{\oplus I}$, that is

$$(\alpha_i) + (\beta_i) \quad := \quad (\alpha_i + \beta_i)$$

Note that $\mathbb{Z}^{\oplus I}$ and $\mathbb{Z}^n$ are commutative, integral monoids, but neither of them is solution-finite. Hence the module of power series over these monoids do not form a well-defined ring.

(7.20) Definition:
Let $(R, +, \cdot)$ be a commutative ring, then we define some abbreviations and slightly different notations for the polynomial and formal power series rings of R over the monoids $\mathbb{N}^{\oplus I}$ and $\mathbb{Z}^{\oplus I}$

- For a non-empty index set $I \neq \emptyset$ we denote the polynomial ring resp. formal power series ring of R over the monoid $\mathbb{N}^{\oplus I}$ and specifically for $I = 1 \dots n$ we also denote the polynomial resp. formal power series ring of R over the monoid $\mathbb{N}^n$ by

$$\begin{aligned} R[t_i \mid i \in I] &:= R[t \mid \mathbb{N}^{\oplus I}] \\ R[t_1, \dots, t_n] &:= R[t \mid \mathbb{N}^n] \\ R[\![t_i \mid i \in I]\!] &:= R[\![t \mid \mathbb{N}^{\oplus I}]\!] \\ R[\![t_1, \dots, t_n]\!] &:= R[\![t \mid \mathbb{N}^n]\!] \end{aligned}$$

 Nota as we have already seen in (7.12) $R[t_i \mid i \in I]$ and $R[\![t_i, \mid i \in I]\!]$ are integral domains, iff the base ring R is an integral domain [as $A = \mathbb{N}^{\oplus I}$ always is integral and solution-finite].

- The symbols t_i in the above two definitions can be given a concrete meaning: Define t_i to be the monomial $t_i := t^{\delta_i}$ where $\delta_i = (\delta_{i,j}) \in \mathbb{N}^{\oplus I}$ then any other monomial t^α where $\alpha = (\alpha_i) \in \mathbb{N}^{\oplus I}$ is a finite product of the form

$$t^\alpha \quad = \quad \prod_{i \in I} t_i^{\alpha_i}$$

 Prob it is clear that $\alpha = \sum_i \alpha_i \delta_i$ and in truth this sum is finite only, as only finitely many $\alpha_i \neq 0$ are non-zero. But since $t^{\alpha+\beta} = t^\alpha t^\beta$ is true for any $\alpha, \beta \in \mathbb{N}^{\oplus I}$ this implies $t^\alpha = \prod_i t^{\alpha_i \delta_i}$ by induction on the number of non-zero α_i. But since $\alpha_i \delta_i = \delta_i + \dots + \delta_i$ (α_i-times) again, we likewise see $t^{\alpha_i \delta_i} = t_i^{\alpha_i}$ by induction the power α_i now. Altogether we found $t^\alpha = \prod_i t^{\alpha_i \delta_i} = \prod_i t_i^{\alpha_i}$.

- Let $I \neq \emptyset$ be a non-empty index set again. Then we denote the polynomial rings over the monoids (even groups) $\mathbb{Z}^{\oplus I}$ and $\mathbb{Z}^n$ by

$$\begin{aligned} R[t_i, t_i^{-1} \mid i \in I] &:= R[t \mid \mathbb{Z}^{\oplus I}] \\ R[t_1, t_1^{-1} \ldots, t_n, t_n^{-1}] &:= R[t \mid \mathbb{Z}^n] \end{aligned}$$

 Nota again we have seen that these rings are integral domains, iff R is an integral domain itself. Note however that the multiplication of the formal power series $R[\![t \mid \mathbb{Z}^{\oplus I}]\!]$ is not well-defined (as $\mathbb{Z}^{\oplus I}$ is *not* solution-finite), even if I is finte. Hence we do not need to introduce the like notation for formal power series over the monoid $\mathbb{Z}^{\oplus I}$.

(7.21) Remark:
The most important case is the polynomial ring $R[t_1, \ldots, t_n]$ in n variables over R, so let us linger and reflect the above definition in this case: First of all the variable symbols t_1 to t_n are maps of the form

$$t_1 \; : \; \mathbb{N}^n \to R \; : \; \alpha \mapsto \begin{cases} 1 \text{ if } \alpha = (1, 0, \ldots, 0) \\ 0 \text{ if else} \end{cases}$$

$$t_n \; : \; \mathbb{N}^n \to R \; : \; \alpha \mapsto \begin{cases} 1 \text{ if } \alpha = (0, \ldots, 0, 1) \\ 0 \text{ if else} \end{cases}$$

Thus by definition of the multiplication of $R[t_1, \ldots, t_n]$ we find the following equality for any multi-index $\alpha = (\alpha_1, \ldots, \alpha) \in \mathbb{N}^n$ (we have just proved this in the definition above)

$$t_1^{\alpha_1} \ldots t_n^{\alpha_n} \;\; = \;\; t^\alpha$$

where $t^\alpha : \mathbb{N}^n \to R$ is the usual map that sends $\alpha \mapsto 1$ and any $\beta \in \mathbb{N}^n$ with $\beta \neq \alpha$ is sent to $\beta \mapsto 0$. Thereby any polynomial $f \in R[t_1, \ldots, t_n]$ can be written, as the following (in truth finite) sum

$$f \;\; = \;\; \sum_{\alpha \in \mathbb{N}^n} f[\alpha]\, t^\alpha \;\; = \;\; \sum_{\alpha_1 = 0}^{\infty} \cdots \sum_{\alpha_n = 0}^{\infty} f[\alpha_1, \ldots, \alpha_n]\, t_1^{\alpha_1} \ldots t_n^{\alpha_n}$$

Any formal power series $f \in R[\![t_1, \ldots, t_n]\!]$ can be written in precisely the same form, but the sum need not be finite in this case. However it is still possible to multiply two such expressions, as the base monoid $\mathbb{N}^n$ is integral and solution finite. So by construction of the polynomial ring $\{\, t^\alpha \mid \alpha \in \mathbb{N}^n \,\}$ is an R-basis of $R[t_1, \ldots, t_n]$, but not a generating set of $R[\![t_1, \ldots, t_n]\!]$. Yet the main difference between polynomials and formal power series becomes apparent, if we try to evaluate f:
If A is a commutative R-algebra and $x_1, \ldots, x_n \in A$ are elements of it, then we can insert these into a polynomial $f \in R[t_1, \ldots, t_n]$, getting a new element of A. Recall that we have already introduced the notation $x^\alpha := x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ early on in (1.41). This notation now fits perfectly, as it allows to rewrite the sum in terms of multi-indices $\alpha = (\alpha_1, \ldots, \alpha) \in \mathbb{N}^n$ again

$$f(x_1, \ldots, x_n) \;\; = \;\; \sum_{\alpha_1 = 0}^{\infty} \cdots \sum_{\alpha_n = 0}^{\infty} f[\alpha_1, \ldots, \alpha_n]\, x_1^{\alpha_1} \ldots x_n^{\alpha_n} \;\; = \;\; \sum_{\alpha \in \mathbb{N}^n} f[\alpha]\, x^\alpha \;\; \in \;\; A$$

Thereby the addition and multiplication of polynomials have been defined precisely in such a way, that $R[t_1,\ldots,t_n] \to A : f \mapsto f(x_1,\ldots,x_n)$ is a homomorphism of R-algebras, according to (7.14). It is *not* possible to insert x_1 to x_n into a formal power series $f \in R[\![t_1,\ldots,t_n]\!]$ though, as in general the sum will not be finite in this case! To do so would require to install a notion of convergence on A and to select those power series for which $f(x_1,\ldots,x_n)$ converges. This is a topic of a course in analysis, by nature.

(7.22) Proposition: (viz. 814)
Let $(R,+,\cdot)$ be a commutative ring, J be an arbitrary index set and $I \subseteq J$ be a subset of J. Then we have a canonical embedding (an R-algebra monomorphism) of the form

$$\begin{array}{rcl} R[t_i \mid i \in I] & \hookrightarrow & R[t_j \mid j \in J] \\ f & \mapsto & \left(\beta \mapsto \begin{cases} f[\beta] & \text{if} \quad \forall\, j \in J \setminus I : \beta(j) = 0 \\ 0 & \text{if} \quad \exists\, j \in J \setminus I : \beta(j) \neq 0 \end{cases} \right) \end{array}$$

And if R is an integral domain and we consider $R[t_i \mid i \in I] \leq_{\mathrm{r}} R[t_j \mid i \in J]$ as a sub-ring under this embedding, then $R[t_i \mid i \in I]$ also is a saturated multiplicatively closed set in $R[t_j \mid j \in J]$. That is for any $f, g \in R[t_j \mid i \in J]$ with $f, g \neq 0$ we have the equivalence

$$f \text{ and } g \in R[t_i \mid i \in I] \iff fg \in R[t_i \mid i \in I]$$

(7.23) Proposition: (viz. 810)

(i) Consider a commutative ring $(R,+,\cdot)$ and any non-empty index set $I \neq \emptyset$. The set of finite subsets of I is denoted by $\Omega(I) := \{\, \omega \subseteq I \mid \#\omega < \infty \,\}$. For any $\omega \in \Omega(I)$ we consider $R[t_i \mid i \in \omega]$ as a subring of $R[t_i \mid i \in I]$, by (7.22). Then any polynomial $f \in R[t_i \mid i \in I]$ is contained in one of the finitely generated subrings $R[t_i \mid i \in \omega]$, and therefore

$$R[t_i \mid i \in I] \;=\; \bigcup_{\omega \in \Omega(I)} R[t_i \mid i \in \omega]$$

(ii) Let $(R,+,\cdot)$ be any commutative ring an fix $1 \geq n \in \mathbb{N}$ and $i, j \in 1 \ldots n$. Then we regard $R[t_1,\ldots,t_j]$ and $R[t_i,\ldots,t_n]$ as sub-rings of $R[t_1,\ldots,t_n]$. And thereby we get

$$R[t_1,\ldots,t_j] \cap R[t_i,\ldots,t_n] \;=\; R[t_i,\ldots,t_j]$$

In particular, iff $j < i$ the only polynomials $f \in R[t_1,\ldots,t_n]$ that lie in both $R[t_1,\ldots,t_j]$ and $R[t_i,\ldots,t_n]$ are the constant ones $f \in R$.

(iii) For any commutative ring $(R,+,\cdot)$ we obtain an epimorphism of R-algebras from the formal power series in arbitrary many variables onto R by evaluation of the *constant term* $f[0]$ of f:

$$\varepsilon \;:\; R[\![t_i \mid i \in I]\!] \twoheadrightarrow R \;:\; f \mapsto f[0]$$

(iv) For any commutative ring $(R,+,\cdot)$ the ring of power series in $n+1$ variables is isomorphic (as an R-algebra) to a ring of power series in 1 variable over a ring of power series in n variables

$$\Phi \;:\; R[\![t_1,t_2,\ldots,t_n]\!][\![t_{n+1}]\!] \quad \cong_{\mathsf{r}} \quad R[\![t_1,t_2,\ldots,t_{n+1}]\!]$$

And this isomorphism Φ is given by $\Phi(f) : \alpha \mapsto f[\alpha_{n+1}]\,[\alpha_1,\alpha_2,\ldots,\alpha_n]$. In particular Φ restricts to an isomorphism between the respective polynomial rings

$$\Phi \;:\; R[t_1,t_2,\ldots t_n][t_{n+1}] \quad \cong_{\mathsf{a}} \quad R[t_1,t_2,\ldots,t_{n+1}]$$

(v) Let again $(R,+,\cdot)$ be a commutative ring and fix any n-tuple of elements $a=(a_1,\ldots,a_n)\in R^n$, then we obtain an R-algebra automorphism on the polynomial ring in n variables by

$$\Phi_a \;:\; R[t_1,t_2,\ldots,t_n] \quad \cong_{\mathsf{r}} \quad R[t_1,t_2,\ldots,t_n] \;:\; f(t)\mapsto f(t+a)$$

(vi) If $(R,+,\cdot)$ is a commutative ring and $a=(a_1,\ldots,a_n)\in R^n$ again, then we also get: Given any $f\in R[t_1,t_2,\ldots,t_n]$ there are some polynomials $q_k\in R[t_1,\ldots,t_k]$ (for $k\in 1\ldots n$) such that f can be written in the following form

$$f(t_1,\ldots,t_n) \;=\; \sum_{k=1}^{n} q_k(t_1,\ldots,t_k)(t_k-a_k)+f(a)$$

(vii) If $(R,+,\cdot)$ is an integral domain then the invertible elements of the polynomial ring in finitely many variables are just the constant polynomials of invertible elements of R

$$R[t_1,\ldots,t_n]^* \;=\; \{\, a\mathbf{1} \mid a\in R^*\,\}$$

(viii) And for any commutative ring $(R,+,\cdot)$ the invertible formal power series in finitely many variables are those whose degree constant term is invertible in R

$$R[\![t_1,\ldots,t_n]\!]^* \;=\; \{\, f\in R[\![t_1,\ldots,t_n]\!] \mid f[0]\in R^*\,\}$$

(7.24) Remark:

- If we are given a formal power series f (in the variable t_{n+1}) over the ring $R[\![t_1,\ldots,t_n]\!]$ of formal power series in the variables t_1 to t_n, then we first express f in the form

$$f=\sum_{\alpha_{n+1}\in\mathbb{N}}\left(\sum_{\alpha\in\mathbb{N}^n} f[\alpha_{n+1}]\,[\alpha_1,\ldots,\alpha_n]\,t_1^{\alpha_1}t_2^{\alpha_2}\ldots t_n^{\alpha_n}\right)t_{n+1}^{\alpha_{n+1}}$$

Using this formal "basis representation" of f the image $\Phi(f)$ under the isomorphism Φ in (ii) simply reads as the following power series in $n+1$ variables:

$$\Phi(f) \;=\; \sum_{\alpha\in\mathbb{N}^{n+1}} f[\alpha_{n+1}]\,[\alpha_1,\ldots,\alpha_n]\,t_1^{\alpha_1}t_2^{\alpha_2}\ldots t_{n+1}^{\alpha_{n+1}}$$

- As $A := R[t_1, \ldots, t_n]$ is an R-algebra, it is clear what we mean by the term $f(t+a)$ for a polynomial $f \in R[t_1, \ldots, t_n]$: Namely $t + a = (t_1 + a_1, \ldots, t_n + a_n)$ is an n-tuple of elements of A and hence we may evaluate f on this tuple, that is

$$f(t+a) \;=\; \sum_{\alpha \in \mathbb{N}^n} f[\alpha]\,(t_1+a_1)^{\alpha_1} \,\ldots\, t_n^{\alpha_n}(t_n+a_n)^{\alpha_n}$$

- The big brother of (7.23.(iv)) is (7.12.(vi)) and if I and J are any non-empty index sets, such that $I \cap J = \emptyset$, [e.g. $I \subseteq K$ and $J := K \setminus I$] then clearly $\mathbb{N}^{\oplus I} \times \mathbb{N}^{\oplus J} = \mathbb{N}^{\oplus (I \cup J)}$. Thus by (7.12.(vi)) we obtain an isomorphism of R-algebras

$$R[s_i \mid i \in I][t_j \mid j \in J] \quad \cong_{\mathrm{r}} \quad R[u_k \mid k \in I \cup J]$$

 And thereby the isomorphism maps t^β to $u^{(0,\beta)}$ and $s^\alpha \mathbf{1} \in R[s_i \mid i \in I][t_j \mid j \in J]$ to $u^{(\alpha,0)}$. The rest is just expansion of this map from the generating elements to the entire ring

$$\sum_{\beta \in \mathbb{N}^{\oplus J}} \left(\sum_{\alpha \in \mathbb{N}^{\oplus I}} f[\beta][\alpha] s^\alpha \right) t^\beta \;\;\mapsto \sum_{(\alpha,\beta) \in \mathbb{N}^{\oplus I} \times \mathbb{N}^{\oplus J}} f[\beta][\alpha] u^{(\alpha,\beta)}$$

 In particular we obtain a canonical embedding of $S := R[s_i \mid i \in I]$ into $R[u_k \mid k \in I \cup J]$, that is an injective monomorphism of rings, by virtue of

$$R[s_i \mid i \in I] \;\hookrightarrow\; R[u_k \mid k \in I \cup J] \;:\; f \mapsto f\mathbf{1}_{S[t_j \mid j \in J]}$$

- In the case of one variable only we can recursively compute the inverse f^{-1} of an invertible power series $f \in R[\![t]\!]^*$ by the following recursion formula. In the case of finitely many variables the inverse of $f \in R[\![t_1, \ldots, t_n]\!]^*$ can be computed sequentially using the isomorphism given in (ii).

$$\begin{aligned} f^{-1}[0] &= f[0]^{-1} \\ f^{-1}[n] &= -f[0]^{-1} \sum_{i=0}^{n-1} f[n-i]\, f^{-1}[i] \end{aligned}$$

(7.25) Definition:
Let $(R, +, \cdot)$ be a commutative ring and regard the polynomial ring in n variables $R[t_1, \ldots, t_n]$. Also fix some *weight* $\omega \in \mathbb{N}^n$ and recall the *weighted sum* of $\alpha \in \mathbb{N}^n$ to be

$$|\alpha|_\omega \;:=\; \omega_1\alpha_1 + \cdots + \omega_n\alpha_n$$

Then for a polynomial $f \in R[t_1, \ldots, t_n]$ we define the **(unordered) degree** $\deg_\omega(f) \in \mathbb{N} \cup -\infty$ of f under the weight $\omega \in \mathbb{N}^n$ to be the maximum weighted sum $|\alpha|_\omega$ among all multi-indices α that contribute a non-zero coefficient $f[\alpha] \neq 0$ to f. Formally, that is

$$\deg_\omega(f) \;:=\; \begin{cases} \max\{\, |\alpha|_\omega \mid \alpha \in \mathbb{N}^n,\, f[\alpha] \neq 0 \,\} & \text{for } f \neq 0 \\ -\infty & \text{for } f = 0 \end{cases}$$

For ease of notation we further introduce some specific unordered degrees of some specific weights ω

$$\begin{array}{rcllcrcl}
\deg(f) & := & \deg_\omega(f) & \text{for} & \omega & := & (1) & = & (1,1,\ldots,1) \\
\deg_j(f) & := & \deg_\omega(f) & \text{for} & \omega & := & (\delta_{i,j}) & = & (0,\ldots,1,\ldots,0) \\
\operatorname{wgt}(f) & := & \deg_\omega(f) & \text{for} & \omega & := & (i) & = & (1,2,\ldots,n)
\end{array}$$

(7.26) Proposition: (viz. 813)
Let R be a commutative ring, $1 \leq n \in \mathbb{N}$ and fix any $\omega \in \mathbb{N}^n$. Then for any $a \in R$ and any two polynomials $f, g \in R[t_1,\ldots,t_n]$ the unordered degree satisfies the following four properties

$$\begin{aligned}
\deg_\omega(at^\alpha) &= \begin{cases} |\alpha|_\omega \text{ if } a \neq 0 \\ -\infty \text{ if } a = 0 \end{cases} \\
\deg_\omega(f) &= \max\{\, \deg_\omega(f[\alpha]t^\alpha) \mid \alpha \in \mathbb{N}^n \,\} \\
\deg_\omega(f+g) &\leq \max\{\, \deg_\omega(f), \deg_\omega(g) \,\} \\
\deg_\omega(f \cdot g) &\leq \deg_\omega(f) + \deg_\omega(g)
\end{aligned}$$

If $\deg_\omega(f) \neq \deg_\omega(g)$ then this even implies the equality in the degree of the sum $f+g$, that is we get $\deg_\omega(f+g) = \max\{\, \deg_\omega(f), \deg_\omega(g) \,\}$. And if R is an integral domain or f or g is monic, then we always have equality of these for the degree of the product $f \cdot g$, that is we get

$$\deg_\omega(f \cdot g) = \deg_\omega(f) + \deg_\omega(g)$$

(7.27) Proposition: (viz. 817)

(i) Let $(R,+,\cdot)$ be an integral domain and consider two polynomials $f, g \in R[t]$ with $f \neq 0$. Then $g(f) \in R[t]$ is another polynomial in $R[t]$ and its degree is given to be

$$\deg\big(g(f)\big) = \deg(f) \cdot \deg(g)$$

(ii) If $(R,+,\cdot)$ is an integral domain again and $f \in R[t_1,\ldots,t_n]$ is a polynomial in $n \in \mathbb{N}$ variables of $\deg(f) \geq 1$ and $g \in R[x]$ is a polynomial in one variable, then we get the equivalence of

$$g(f) = 0 \iff g = 0$$

Now let $(R,+,\cdot)$ be a commutative ring, $I \neq \emptyset$ an index set and denote $A := R[t_i \mid i \in I]$ the polynomial ring. We consider $R \subseteq A : a \mapsto a\mathbf{1}$ canonically. Then we obtain the following statements

(iii) Any $p \in R$ is prime in R if and only if $p = p\mathbf{1} \in A$ is prime, that is: $p \in R$ prime $\iff$ $p \in A$ prime.

(iv) Let R be an integral domain and fix $i \in I$ and $a_i \in R$, then $t_i - a_i \in A$ is a prime element of A.

(v) Once more let R be an integral domain and fix any $i \in I$, then $t_i A \trianglelefteq_{\mathrm{i}} A$ is a minimal prime ideal over $0 \trianglelefteq_{\mathrm{i}} A$. That is for any prime ideal $\mathfrak{p} \trianglelefteq_{\mathrm{i}} A$ we have the implication

$$0 \subseteq \mathfrak{p} \subseteq t_i A \implies \mathfrak{p} = 0 \text{ or } \mathfrak{p} = t_i A$$

(7.28) Proposition: (viz. 814)
Let $(R,+,\cdot)$ be a commutative ring and $f \in R[t_1,\ldots,t_n]$ be a polynomial in $1 \leq n \in \mathbb{N}$ variables. Then there are polynomials $f_1,\ldots,f_n$ such that (for any $k \in 1\ldots n$) we get (1) $f_k \in R[t_1,\ldots,t_k]$ and (2) $\deg(f_k) < \deg(f)$ and (3) f has a decomposition in the following form

$$f \;=\; f(0) + \sum_{k=1}^{n} f_k(t_1,\ldots,t_k)t_k$$

In particular the polynomial ring $R[t_1,\ldots,t_n]$ can be decomposed into $R\,\mathbf{1}$ and a sum of prime ideals

$$R[t_1,\ldots,t_n] \;=\; R\,\mathbf{1} + \sum_{k=1}^{n} t_k R[t_1,\ldots,t_n]$$

(7.29) Lemma: (viz. 820)
Let $(R,+,\cdot)$ be an UFD, denote its quotient field by $E := \mathrm{QUOT}(R)$, and consider $R \subseteq E : a \mapsto a/1$ canonically. Also let $I \neq \emptyset$ be any index set and denote the polynomial rings $A := R[t_i \mid i \in I]$ and $B := E[t_i \mid i \in I]$. In particular $A \subseteq B$. We also consider $R \subseteq A : a \mapsto a\mathbf{1}$ canonically. Finally recall (5.26) where $f \in A$ was said to be *primitive* iff $f \neq 0$ and $1 \in \mathrm{cont}(f)$. Thereby the *content* of $f \in A$ (as an element of a free module) has been defined to be

$$\mathrm{cont}(f) \;=\; \gcd\{\, f[\alpha] \mid \alpha \in \mathbb{N}^{\oplus I},\, f[\alpha] \neq 0 \,\}$$

(i) Consider $a \in R$ and $f \in A$, then a divides f (in A) if and only if a divides the content $\mathrm{cont}(f)$ of f (in R). That is for any $c \in \mathrm{cont}(f)$ we have the following equivalence of

$$a \mid c \;\text{ in } R \quad\Longleftrightarrow\quad a \mid f \;\text{ in } A$$

(ii) For any polynomial $f \in A$ and any $c \in R$ we find that c is the content of f if and only iff $f = cf_1$ for some primitive polynomial $f_1 \in A$

$$c \in \mathrm{cont}(f) \quad\Longleftrightarrow\quad \exists\, f_1 \in A \;:\; f = cf_1 \;\text{ and }\; f_1 \;\text{ primitive}$$

(iii) If $u \in B$ with $u \neq 0$ is a non-zero polynomial over the quotient field E, then there are some a, $b \in R \setminus \{0\}$ and a primitive polynomial $u_1 \in A$ such that u can be written, as

$$u \;=\; \frac{a}{b}u_1$$

(iv) The content of polynomials is multiplicative. That is for any polynomials $f, g \in A$ with $c \in \mathrm{cont}(f)$ and $d \in \mathrm{cont}(g)$ we have $cd \in \mathrm{cont}(fg)$. In particular the set $U := \{\, f \in A \mid f \text{ primitive} \,\}$ of primitive polynomials is a multiplicatively closed set in A.

(v) Let us abbreviate either the word *primitive* or *monic* by $\star$ and consider $u, v \in E[t]$ any polynomials over E, such that the product $uv \in E[t]$ in fact is a $\star$ polynomial of $R[t]$, formally

$$uv \in R[t] \;\text{ and }\; uv \text{ is } \star$$

Then there are a, b, c and $d \in R \setminus \{0\}$ and polynomials u_1, $v_1 \in R[t]$ that satisfy the properties

(1) u and $v \in R[t]$ are $\star$

(2) $u = \frac{a}{b}u_1$ and $v = \frac{c}{d}v_1$

(3) $uv = u_1v_1$

(vi) If $p \in A$ is primitive and $f \in A$ is any polynomial then p divides f in A if and only if p divides f in B - that is the equivalence given below. In fact, if $f = pq$ for some $q \in B$, then $q \in A$ already.

$$p \mid f \text{ in } A \iff p \mid f \text{ in } B$$

(vii) Let $p \in A \setminus R$ be primitive and let $\star$ abbreviate one of the words *prime* or *irreducible*. Then $p \in A$ is $\star$ in A if and only if it is $\star$ in B, formally again

$$p \in A \text{ is } \star \iff f \in B \text{ is } \star$$

(viii) *Lemma of Gauss*: If the base ring R is a factorial domain, then the polynomial ring A is a factorial domain, too and vice versa. That is the following equivalence

$$R \text{ is an UFD} \iff A \text{ is an UFD}$$

Laurent Series

Until now we have regarded polynomial rings $R[t]$, formal series $R[\![t]\!]$ and even $R[t, t^{-1}]$. In complex analysis and p-adic analysis there even occur mixtures of these structures - so called Laurent series. We are not particularly interested in them, but they are important enough to not go unmentioned here.

(7.30) Proposition: (viz. 824)

Let $(R, +, \cdot)$ be a commutative ring, fix a natural number $1 \leq n \in \mathbb{N}$ and let us abbreviate the module $M := R[\![t \mid \mathbb{Z}^n]\!]$ of formal power series over $\mathbb{Z}^n$ with coefficients in R. Then we introduce the notions

(i) A formal power series $f \in M$ is said to be a **(formal) Laurent series**, iff its negative powers do not drop indefinitely, i.e. they don't proceed below some finite degree ℓ. Formally that is:

$$\exists\, \ell \in \mathbb{Z} \;:\; \forall\, \alpha \in \mathbb{Z}^n \text{ with } f[\alpha] \neq 0 \text{ we get } \forall\, i \in 1 \ldots n \;:\; \ell \leq \alpha_i$$

The set $L := \{\, f \in M \mid f \text{ is a formal Laurent series} \,\}$ of all Laurent series is a sub-module of M. In fact it even becomes a commutative ring under the usual multiplication

$$\left(\sum_{\alpha \in \mathbb{Z}^n} f[\alpha] t^\alpha \right) \cdot \left(\sum_{\beta \in \mathbb{Z}^n} g[\beta] t^\beta \right) \;=\; \sum_{\gamma \in \mathbb{Z}^n} \left(\sum_{\alpha+\beta=\gamma} f[\alpha]\, g[\beta] \right) t^\gamma$$

(ii) This construction allows us to define the order of a formal laurent series $f \in L$ (where $f \neq 0$). Fix some weight $\omega \in \mathbb{N}^n$ and define the **(weighted) order** of f to be the minimal weight of an non-zero coefficient of f, formally that is

$$\operatorname{ord}_\omega(f) \;:=\; \min\{\, |\alpha|_\omega \mid \alpha \in \mathbb{Z}^n,\ f[\alpha] \neq 0 \,\}$$

If such an index does not exist, i.e. in the case $f \in M \setminus L$ we formally take the order to be $\operatorname{ord}_\omega(f) := -\infty$ and as a very special case, we let $\operatorname{ord}_\omega(0) := \infty$.

(iii) The weighted order on L has most of the properties of a valuation: It is sub-additive and sub-multiplicative. I.e. for any $\omega \in \mathbb{N}^n$ and any two Laurent series $f, g \in L$ we get

$$\begin{aligned} \operatorname{ord}_\omega(f) + \operatorname{ord}_\omega(g) &\leq \operatorname{ord}_\omega(f\,g) \\ \min\{\, \operatorname{ord}_\omega(f), \operatorname{ord}_\omega(f) \,\} &\leq \operatorname{ord}_\omega(f+g) \\ \operatorname{ord}_\omega(-f) &= \operatorname{ord}_\omega(f) \end{aligned}$$

And if R is an integral domain, then the order even is multiplicative, that is we get the property

$$\operatorname{ord}_\omega(f\,g) \;=\; \operatorname{ord}_\omega(f) + \operatorname{ord}_\omega(g)$$

(iv) Let us abbreviate the ring of formal power series by $P := R[\![t \mid \mathbb{N}^n]\!]$. Then the subset of monoids $U = \{\, t^\alpha \mid \alpha \in \mathbb{N}^n \,\} \subseteq P$ is multiplicatively closed and the ring of formal Laurent series is isomorphic to the localization of P in U, formally

$$U^{-1}P \;\cong_{\mathrm{r}}\; L \;:\; \frac{f}{t^\alpha} \;\mapsto\; t^{-\alpha} f$$

(v) In the case $n = 1$, if R is a field we even get the following isomorphy between the quotient field of $R[\![t]\!]$ and the ring of formal Laurent series $L = R[\![t]\!][t^{-1}]$ by virtue of (where $\operatorname{ord} := \operatorname{ord}_{(1)}$)

$$\textsc{quot}\big(R[\![t]\!]\big) \;\cong_{\mathrm{f}}\; R[\![t]\!][t^{-1}] \;:\; \frac{f}{g} \;\mapsto\; t^{-\operatorname{ord}(f)} f \cdot (t^{-\operatorname{ord}(g)} g)^{-1}$$

Space of Arcs

We conclude this subsection by regarding powers and products of formal power series in one variable. We will compute an explicit formula for $f(a_1, \ldots, a_n)$ and study how the higher powers depend on the powers of the a_i. This is interesting for expansions of analytic functions as power series and for spaces of arcs on affine varieties. The letter is a method of analysing the higher-order curvature of an affine variety, much like a Taylor expansion analyses the curvature of a function. It is a little technical and not required to understand the rest of this textbook.

(7.31) Definition:
We fix $1 \leq n \in \mathbb{N}$ and consider any commutative ring $(R, +, \cdot)$, a polynomial $f \in R[t_1, \ldots, t_n]$ in n variables and n formal power series $a_1, \ldots, a_n \in R[\![\varepsilon]\!]$ in one variable ε over over R

$$\begin{aligned} f(t_1, \ldots, t_n) &= \sum_{\alpha \in \mathbb{N}^n} f[\alpha]\, t^\alpha \\ a_i(\varepsilon) &= \sum_{j=0}^{\infty} a_i[j]\, \varepsilon^j \end{aligned}$$

Let us denote the n-tuple $a := (a_1, \ldots, a_n) \in R[\![\varepsilon]\!]^n$ then we want to deprive a of its algebraic structure and only store the coefficients of the series a_i in the following form: Let $a[k] := (a_1[k], \ldots, a_n[k]) \in R^n$ for any $k \in \mathbb{N}$ and also define

$$\dot{a} \;:=\; (a[0],\, a[1],\, a[2],\, \ldots) \;\in\; \left(R^n\right)^{\mathbb{N}}$$

In the following, for any $k \in \mathbb{N}$, we want to define a function $\mathcal{L}_k$ that assigns a polynomial in the variables $t_{i,j}$, where $i \in 1 \ldots n$ and $j \in \mathbb{N}$ to a given polynomial $f \in R[t_1, \ldots, t_n]$. This will require some preparations, though: First of all, let us denote

$$\begin{aligned} B &:= \left(\mathbb{N}^{\oplus\mathbb{N}}\right)^n \\ P_n &:= R\left[t_{i,j} \mid i \in 1 \ldots n,\, j \in \mathbb{N}\right] \end{aligned}$$

Recall that $|\alpha| := \alpha_1 + \cdots + \alpha_n$ for a multi-index $\alpha \in \mathbb{N}^n$. We now need to transfer this notation to the case of multi-multi-indices. That is for $\beta = (\beta_1, \ldots, \beta_n) \in B$ we further define the following notations (where $\beta_i = (\beta_{i,0}, \beta_{i,1}, \beta_{i,2}, \ldots) \in \mathbb{N}^{\oplus\mathbb{N}}$)

$$|\beta| \;:=\; \left(\sum_{j=0}^{\infty} \beta_{1,j}, \ldots, \sum_{j=0}^{\infty} \beta_{n,j}\right) \;\in\; \mathbb{N}^n$$

$$\|\beta\| \;:=\; \sum_{i=1}^{n} \sum_{j=0}^{\infty} j\beta_{i,j} \;\in\; \mathbb{N}$$

As any β_i only has finitely many non-zero entries $\beta_{i,j} \neq 0$ the same is true for β and also $|\beta|$ and $\|\beta\|$ are well-defined. In fact, if if $\beta_{i,j} \neq 0$, then $\|\beta\| \geq j$ and hence we get $\beta_{i,j} = 0$ for any $i \in 1 \ldots n$ and $j > \|\beta\|$. Therefore for any $\alpha \in \mathbb{N}^n$ and any $k \in \mathbb{N}$ the following subset of B is finite

$$B(\alpha, k) \;:=\; \{\, \beta \in B \mid |\beta| = \alpha,\ \|\beta\| = k \,\}$$

If now $\beta \in B$ (as above) and $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ satisfy $|\beta| = \alpha$ then we may define the binomial coefficient of α over β to be the following (note that the product in truth is finite, as $\beta_{i,j} = 0$ for all but finitely many $i \in 1 \ldots n$ and $j \in \mathbb{N}$, such that $\beta_{i,j}! = 1$ in this case)

$$\binom{\alpha}{\beta} \;:=\; \prod_{i=1}^{n} \binom{\alpha_i}{\beta_i} \;=\; \prod_{i=1}^{n} \alpha_i! \left(\prod_{j=0}^{\infty} \beta_{i,j}!\right)^{-1} \;\in\; \mathbb{N}$$

Finally consider some sequence $\dot{a} = (a_{i,j})$ where $a_{i,j} \in R$ and $i \in 1 \ldots n$, $j \in \mathbb{N}$ and let $\beta \in B$ be as

above. Then we generalize our notation of powers by multi-indices somewhat, to

$$t^\beta \;:=\; \prod_{i=1}^{n}\prod_{j=0}^{\infty} t_{i,j}^{\beta_{i,j}} \;\in\; P_n$$

$$\dot{a}^\beta \;:=\; \prod_{i=1}^{n}\prod_{j=0}^{\infty} a_{i,j}^{\beta_{i,j}} \;\in\; R$$

Using these notations let us define the function $\mathcal{L}_k : R[t_1,\ldots,t_n] \to P_n$ for any $k \in \mathbb{N}$ to be (note that this truly is a polynomial, as $f[\alpha] = 0$ for all but finitely many $\alpha \in \mathbb{N}^n$ and $B(\alpha,k)$ is a finite set)

$$\mathcal{L}_k(f) \;:=\; \sum_{\alpha\in\mathbb{N}^n}\sum_{\beta\in B(\alpha,k)} \binom{\alpha}{\beta} f[\alpha]\, t^\beta \;\in\; P_n$$

Nota and as $\beta_{i,j} = 0$ for any $j > \|\,\beta\,\| = k$ the polynomial $\mathcal{L}_k(f) \in P_n$ does not contain any of the variables $t_{i,j}$ whenever $j > k$. In other words $\mathcal{L}_k(f)$ is contained in the following sub-ring of P_n

$$\mathcal{L}_k(f) \;\in\; R[t_{i,j} \mid i \in 1\ldots n,\, j \in 0\ldots k]$$

(7.32) Proposition: (viz. 833)
Fix $n \in \mathbb{N}$ and let $a(\varepsilon), a_1(\varepsilon), \ldots, a_n(\varepsilon) \in R[\![\varepsilon]\!]$ be formal power series in one variable over the commutative ring R and let $f, g \in R[t_1,\ldots,t_n]$ be polynomials in n variables over R.

(i) Let $b_1(\varepsilon),\ldots,b_n(\varepsilon) \in R[\![\varepsilon]\!]$ be further formal power series such that b_i is identical to a_i up to some degree $l \in \mathbb{N}$, i.e. for all $i \in 1\ldots n$ and $k \in 0\ldots l$ we have $a_i[k] = b_i[k]$. Then $f(a_1,\ldots,a_n)$ and $f(b_1,\ldots,b_n)$ agree up to degree l as well:

$$\forall\, k \in 0\ldots l \quad \text{we get} \quad f(a_1,\ldots,a_n)[k] \;=\; f(b_1,\ldots,b_n)[k]$$

(ii) For a general polynomial $f \in R[t_1,\ldots,t_n]$ we use the notations of (7.31) introduced above and thereby obtain the expression

$$f(a_1,\ldots,a_n)(\varepsilon) \;=\; \sum_{k=0}^{\infty} \mathcal{L}_k(f)(\dot{a})\,\varepsilon^k$$

(iii) Then the map $f \mapsto \mathcal{L}_k(f)$ from $R[t_1,\ldots,t_n]$ to $R[t_{i,j} \mid i \in 1\ldots n,\, j \in 0\ldots k]$ clearly is R-linear and satisfies the following multiplicative property for any $f, g \in R[t_1,\ldots,t_n]$

$$\mathcal{L}_k(f\cdot g) \;=\; \sum_{i+k=k} \mathcal{L}_i(f)\cdot\mathcal{L}_j(g)$$

(iv) Suppose the $a_j(t)$ are of degree $l-1$ only, i.e. we regard the polynomials a_j and consider these polynomials with another (the l-th) term appended

$$\begin{aligned} a_j(\varepsilon) &= a_j[0] + a_j[1]\varepsilon + \cdots + a_j[l-1]\varepsilon^{l-1} \\ \overline{a}_j(\varepsilon) &:= a_j(\varepsilon) + a_j[l]\varepsilon^l \end{aligned}$$

Let $\partial_j f$ denote the formal derivative of f to the j-th variable t_j then the l-th coefficient of the evaluated expression $f(\overline{a}_1,\dots,\overline{a}_n)(\varepsilon)$ is modified as follows:

$$f(\overline{a})[l] \;=\; f(a)[l] + \sum_{j=1}^{n} (\partial_j f)(a[0]) \cdot a_j[l]$$

(7.33) Remark:
By construction $\mathcal{L}_k(f)$ is a polynomial in $P_n = R[t_{i,j} \mid i \in 1\dots n,\, j \in \mathbb{N}]$ in which no $t_{i,j}$ with $j > k$ appears. This is the reason why we may consider $\mathcal{L}_k(f) \in R[t_{i,j} \mid i \in 1\dots n,\, j \in 0\dots k]$ which we regard as a sub-ring of P_n. Therefore, if we evaluate $\mathcal{L}_k(f)$ on $\dot{a} = (a[0], a[1], a[2], \dots)$ in $\mathcal{L}_k(f)(\dot{a})$ there does not appear any coefficient $a_i[j] = t_{i,j}(\dot{a})$ for any index $j > k$. Hence we may omit $a[j]$ for any $j > k$ as in truth $\mathcal{L}_k(f)(\dot{a})$ only depends on $a[0]$ to $a[k]$

$$\mathcal{L}_k(f)\big(a[0], a[1], a[2], \dots\big) \;=\; \mathcal{L}_k(f)\big(a[0], a[1], \dots, a[k]\big)$$

(7.34) Example:
Let R be a commutative ring and consider the polynomial $f(t_1, t_2) := t_1^2 + t_2^2 - r^2$ defining a circle X of radius r around the origin of R^2. Also let $a_1 := a_1[0] + a_1[1]\varepsilon$ and $a_2 := a_2[0] + a_2[1]\varepsilon$ and append $\overline{a}_1 := a_1 + a_1[2]\varepsilon^2$ and $\overline{a}_2 := a_2 + a_2[2]\varepsilon^2$ respectively. Then an elementary computation yields

$$\begin{aligned}
f\big(a_1, a_2\big) \;&=\; \big(a_1[0]^2 + a_2[0]^2 - r^2\big) \\
&\quad + 2\big(a_1[0]a_1[1] + a_2[0]a_2[1]\big)\varepsilon \\
&\quad + \big(a_1[1]^2 + a_2[1]^2\big)\varepsilon^2 \\
f\big(\overline{a}_1, \overline{a}_2\big) \;&=\; \big(a_1[0]^2 + a_2[0]^2 - r^2\big) \\
&\quad + 2\big(a_1[0]a_1[1] + a_2[0]a_2[1]\big)\varepsilon \\
&\quad + \big(a_1[1]^2 + 2a_1[0]a_1[2] + 2a_2[0]a_2[2] + a_2[1]^2\big)\varepsilon^2 \\
&\quad + 2\big(a_1[1]a_1[2] + a_2[1]a_2[2]\big)\varepsilon^3 \\
&\quad + \big(a_1[2]^2 + a_2[2]^2\big)\varepsilon^4
\end{aligned}$$

From this we see that $f(a_1, a_2)$ and $f(\overline{a}_1, \overline{a}_2)$ share the same coefficients for $k = 0$ and $k = 1$, as predicted in (i). And for $k = 2$ we have $\partial_1 f = 2t_1$, such that $(\partial_1 f)(a[0]) \cdot a_1[2] = 2a_1[0]a_1[2]$, likewise $(\partial_2 f)(a[0]) \cdot a_2[2] = 2a_2[0]a_2[2]$. So, as predicted in (iv), we truly have

$$f\big(\overline{a}_1, \overline{a}_2\big)[2] \;=\; f\big(a_1, a_2\big)[2] + (\partial_1 f)(a[0]) \cdot a_1[2] + (\partial_2 f)(a[0]) \cdot a_2[2]$$

7.4 Graded Algebras

(7.35) Definition:
Let $(D,+)$ be a commutative monoid and $(R,+,\cdot)$ be a commutative ring. Then the ordered pair $(A,\deg)$ is said to be a D**-graded** R**-(semi)algebra**, iff it satisfies all of the following properties

(1) A is a commutative R-(semi)algebra

(2) $\deg : A_{\text{hom}} \to D$ is a function from some subset $A_{\text{hom}} \subseteq A$ to D, where we require $0 \notin A_{\text{hom}}$. Thereby an element $h \in A$ is said to be **homogeneous**, iff $h \in A_{\text{hom}} \cup \{0\}$.

(3) For any $d \in D$ let us denote $A_d := \deg^{-1}(d) \cup \{0\} \subseteq A$. Then we require that $A_d \leq_{\mathfrak{m}} A$ is an R-sub-module of A and that A is decomposed as an inner direct sum of sub-modules

$$A \;=\; \bigoplus_{d\in D} A_d$$

(4) Given any c, $d \in D$ we require that the product gh of the homogeneous elements g of degree c and h of degree d is a homogeneous element of degree $c+d$. That is: If we define the set of products $A_cA_d := \{\, gh \mid g \in A_c, h \in A_d \,\}$, then we require

$$A_cA_d \;\subseteq\; A_{c+d}$$

(7.36) Remark:

- By property (2) A_d is a sub-module of A, that is the sum $g+h$ of two homogeneous elements of degree d again is a homogeneous element of degree d. And likewise the scalar multiple ah is a homogeneous element of degree d as well. Thus for any g, $h \in A_{\text{hom}}$ with $\deg(g) = \deg(h)$ and any $a \in R$ such that $ag+h \neq 0$ we get

$$\deg(ag+h) \;=\; \deg(g) \;=\; \deg(h)$$

- Property (4) asserts that the product of homogeneous elements is homogeneous again, in particular $A_{\text{hom}} \cup \{0\}$ is closed under multiplication. And thereby the degree even is additive, that is for any two homogeneous elements g, $h \in A_{\text{hom}}$ we get

$$gh \neq 0 \quad\Longrightarrow\quad \deg(gh) = \deg(g) + \deg(h)$$

- According to (3) any element $f \in A$ has a unique decomposition in terms of homogeneous elements. To be precise, given any $f \in A$, there is a uniquely determined sequence of elements (f_d) (where $d \in D$) such that $f_d \in A_d$ (that is $f_d = 0$ or $\deg(f_d) = d$) the set $\{\, d \in D \mid f_d \neq 0 \,\}$ is finite and

$$f \;=\; \sum_{d\in D} f_d$$

 Thereby f_d is called the **homogeneous component** of degree d of f. And writing $f = \sum_d f_d$ we will often speak of the decomposition of f into homogeneous components.

- It is unsatisfactory to always distinguish the cases $h = 0$ when considering a homogeneous element $h \in A_{\text{hom}} \cup \{0\} \subseteq A$. Hence we will add the symbol $-\infty$ to D as outlined in (7.4). Then the degree can be extended canonically to all homogeneous elements

$$\deg \ : \ A_{\text{hom}} \cup \{0\} \to D \cup \{-\infty\} \ : \ h \mapsto \begin{cases} \deg(h) \text{ if } h \neq 0 \\ -\infty \text{ if } h = 0 \end{cases}$$

 If A is an integral domain this turns "deg" into a homomorphism of semigroups, from $A_{\text{hom}} \cup \{0\}$ (under the multiplication of A) to D. That is for any $g, h \in A_{\text{hom}} \cup \{0\}$ we now get

$$\deg(gh) \ = \ \deg(g) + \deg(h)$$

- In the literature it is customary to call the decomposition $A = \bigoplus_d A_d$ itself a D-graded R-algebra, supposed $A_c A_d \subseteq A_{c+d}$. But this clearly is equivalent to the definition we gave here. Just let

$$A_{\text{hom}} \ := \ \bigcup_{d \in D} A_d \setminus \{0\}$$

 Then we obtain a well-defined function $\deg : A_{\text{hom}} \to D$ by letting $\deg(h) := d$ where $d \in D$ is (uniquely) determined by $h \in A_d$. And thereby it is clear that $(A, \deg)$ becomes a D-graded R-algebra, with $\deg^{-1}(d) = A_d \setminus \{0\}$ again.

(7.37) Example:
If $(R, +, \cdot)$ is any commutative ring and $(D, +)$ is any commutative monoid (with neutral element 0), then there is a trivial construction turning R into a D-graded R-algebra. Just let $R_{\text{hom}} := R \setminus \{0\}$ and define the degree by $\deg : R_{\text{hom}} \to D : h \mapsto 0$. That is $R_0 = R$, whereas $R_d = 0$ for any $d \neq 0$. Thus examples of graded algebras abound, but of course this construction won't produce any new insights.

(7.38) Remark:
Given some commutative ring $(A, +, \cdot)$ [and a commutative monoid $(D, +)$] there are two canonical ways how to regard A as an R-algebra

(1) We could fix $R := A$, in this case the sub-modules $A_d \ \leq_{\mathfrak{m}} \ A$ occurring in property (3) would be ideals $A_d \ \trianglelefteq_{\mathfrak{i}} \ A$. So this would yield a quite peculiar property: As A_d is an ideal we have $A_c A_d \subseteq A_d$ but also $A_c A_d \subseteq A_{c+d}$ by property (4). But if $c + d \neq d$ then $A_{c+d} \cap A_d = \{0\}$ such that $A_c A_d = 0$. So homogeneous elements of non-zero degree have to delete each other by multiplication.

(2) Secondly we could fix $R := \mathbb{Z}$, in this case the sub-modules $A_d \ \leq_{\mathfrak{m}} \ A$ occuring in property (3) would only have to be subgroups $A_d \ \leq_{\mathfrak{g}} \ A$. Thus there no longer is a reference to the algebra structure of A. Hence we will also speak of a *D-graded ring* in this case.

(7.39) Example:
The classical example and the sole reason for the entire concept of graded algebras, is the following: Let $(R,+,\cdot)$ be any commutative ring, fix any $1 \leq n \in \mathbb{N}$ and let $A := R[t_1,\ldots,t_n]$ be the polynomial ring in n variables. Recall that the (standard) *degree* of a polynomial $f \in A$ with $f \neq 0$ is defined to be

$$\deg(f) \quad = \quad \max\{\, |\alpha| \mid \alpha \in \mathbb{N}^n,\, f[\alpha] \neq 0 \,\}$$

Now a polynomial $f \in A$ with $f \neq 0$ and $d := \deg(f) \in \mathbb{N}$ is said to be **homogeneous** iff all its monomials are of degree d. That is iff for any $\alpha \in \mathbb{N}^n$ we have the implication

$$f[\alpha] \neq 0 \quad \Longrightarrow \quad |\alpha| = d$$

In particular any monomial is homogeneous. Also $t_1^2 t_2^2 t_3 + t_1 t_3^4$ is an example of a homogeneous polynomial of degree 5. Yet $t_1 + t_1^3 \in R[t_1]$ is not homogeneous, as its monomials have different degree. Thereby the homogeneous polynomials of degree d (apart from 0) form the set

$$A_d \quad = \quad \mathrm{Lh}_R\{\, t^\alpha \in A \mid \alpha \in \mathbb{N}^n,\, |\alpha| = d \,\}$$

Thereby A becomes an $\mathbb{N}$-graded R-algebra, as all the A_d are sub-modules of R, that satisfy the multiplicative property $A_c A_d \subseteq A_{c+d}$ and A is the inner direct sum

$$A \quad = \quad \bigoplus_{d\in\mathbb{N}} A_d$$

(7.40) Proposition: (viz. 784)
Let $(R,+,\cdot)$ be a commutative ring m, $n \in \mathbb{N}$ where $n \geq 1$ and consider a polynomial $f \in R[t_1,\ldots,t_n]$, that is non-zero $f \neq 0$. Let $d := \deg_n(f)$ be the degree of x_n in f (that is the highest power of x_n occurring). Then the following two statements are equivalent

(a) f is a homogeneous polynomial of degree $m = \deg(f)$

(b) f can be written in the following form, where for any $k \in 0\ldots d$ any polynomial $f_k \in R[t_1,\ldots,t_{n-1}]$ is homogeneous of degree $\deg(f_k) = m - k$ or $f_k = 0$:

$$f(t_1,\ldots,t_n) \quad = \quad \sum_{k=0}^{d} f_k(t_1,\ldots,t_{n-1})\, t_n^k$$

In this case $f_d \neq 0$ is non-zero. For a general polynomial f, we can still write f in the form given in (b), but the f_k need not be homogeneous and only need to have $\deg(f_k) \leq m - k$.

Rees Algebra

The following construction will be twofold: For one we see that an ideal $\mathfrak{a}$ induces a metric on R, that turns R into a topological ring, if the intersection of the powers $\mathfrak{a}^n$ is zero. This construction is used in p-adic analysis, for example. And for a general ideal we can define the *Rees-algebra*, which is a $\mathbb{N}$-graded algebra. In case the intersection of the $\mathfrak{a}^n$ is zero, we can introduce a canonical map from R to the Rees-algebra. The Rees-algebra will later play a role in several theories like the Hilbert-Samuel polynomial and dimension theory of rings (in particular regular local rings).

(7.41) Definition:

Let $(R,+,\cdot)$ be a commutative ring and $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be an ideal of R, then we say that $\mathfrak{a}$ is a **filter-ideal**, iff the intersection of all powers $\mathfrak{a}^n$ of $\mathfrak{a}$ is the zero-ideal (where for $n = 0$ we take $\mathfrak{a}^n := R$), that is

$$\bigcap_{n\in\mathbb{N}} \mathfrak{a}^n \;=\; \{0\}$$

Then it is clear, that any $a \in R$ with $a \neq 0$ is contained in a maximal power $\mathfrak{a}^n$ of the ideal $\mathfrak{a}$. And thereby we may define the **order** $\mathrm{ord}(a)$ of a to be that maximal power

$$\mathrm{ord} \;:\; R\setminus\{0\} \to \mathbb{N} \;:\; a \mapsto \max\Big\{\, k\in\mathbb{N} \mid a \in \mathfrak{a}^k \,\Big\}$$

Specifically for $a = 0$ we define $\mathrm{ord}(a) := \infty$. Then this map is well-defined, but need neither be additive, nor multiplicative. However it is super-additive and super-multiplicative, that is for any a, $b \in R$ we have

(1) $\mathrm{ord}(a+b) \;\geq\; \min\{\,\mathrm{ord}(a), \mathrm{ord}(b)\,\}$

(2) $\mathrm{ord}(ab) \;\geq\; \mathrm{ord}(a)\cdot\mathrm{ord}(b)$

Prob If $m = \mathrm{ord}(a)$ and $n = \mathrm{ord}(b)$ then $a \in \mathfrak{a}^m$ and $b \in \mathfrak{a}^n$ such that $ab \in \mathfrak{a}^m \cdot \mathfrak{a}^n = \mathfrak{a}^{m+n}$. In particular $\mathrm{ord}(ab) \geq m+n = \mathrm{ord}(a) + \mathrm{ord}(b)$. We may assume $m \leq n$, else interchange a and b. Then $\mathfrak{a}^n \subseteq \mathfrak{a}^m$ such that both, a and $b \in \mathfrak{a}^m$. In particular $a+b \in \mathfrak{a}^m$ such that $\mathrm{ord}(a+b) \geq m = \min\{\,\mathrm{ord}(a), \mathrm{ord}(b)\,\}$.

(7.42) Remark: (viz. 788)

Let $(R,+,\cdot)$ be a commutative ring and $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be filter-ideal. Note that for any ideal $(\mathfrak{a},+)$ is a subgroup of the additive group $(R,+)$ of R. And thereby (6.41) tells us, that we get a metric d on R by taking $d(a,b) := 0$ for $a = b$ and for $a \neq b$ we have to define

$$d(a,b) \;:=\; \frac{1}{2^n} \quad \text{where} \quad n \;:=\; \mathrm{ord}(a-b)$$

In case of doubt we also write $d_{\mathfrak{a}}(a,b)$ for this metric. Recall that being a metric includes the symmetry and triangle inequality. That is for any a, b and $c \in R$ we get

(1) $d(a,b) \;=\; d(b,a)$

(2) $d(a,c) \;\leq\; d(a,b) + d(b,c)$

As always $(R,+)$ becomes a topological group, but in this case $(R,+,\cdot)$ even is a *topological ring*, that is $R\times R\to R:(a,b)\mapsto ab$ is continuous, too. In this so called $\mathfrak{a}$-*adic* topology on R, a set $U\subseteq R$ is said to be *open*, iff it satisfies the following property

$$U\subseteq R \text{ open} \iff \forall\, u\in U\ \exists\, n\in\mathbb{N}\ :\ u+\mathfrak{a}^n\subseteq U$$

Nota that the multiplication $(a,b)\mapsto ab$ of R is continuous can be translated in the following way: For any open set $W\subseteq R$ and any $a,b\in R$ with $ab\in W$ there are some open neighbourhoods $U\in\mathcal{T}(a)$ and $V\in\mathcal{T}(b)$ such that for any $u\in U$ and any $v\in V$ we have $uv\in W$ again.

(7.43) Definition:
Let $(R,+,\cdot)$ be a commutative ring and $\mathfrak{a}\trianglelefteq_{\mathfrak{i}} R$ be an ideal of R. Note that for any $n\in\mathbb{N}$ the quotient $\mathfrak{a}^n/\mathfrak{a}^{n+1}$ becomes an $R/\mathfrak{a}$-module under the scalar multiplication $(a+\mathfrak{a})(f+\mathfrak{a}^{n+1}):=(af+\mathfrak{a}^{n+1})$ which is well-defined. Let us now take to the exterior direct sum of these $R/\mathfrak{a}$-modules

$$R(\mathfrak{a}) \ :=\ \bigoplus_{n\in\mathbb{N}} \mathfrak{a}^n\Big/\mathfrak{a}^{n+1}$$

Therefore $R(\mathfrak{a})$ can be turned into an $R/\mathfrak{a}$-algebra (the so called *Rees-algebra* of R in $\mathfrak{a}$), by defining the following scalar multiplication and multiplication

$$\begin{aligned}(a+\mathfrak{a})\left(f_n+\mathfrak{a}^{n+1}\right) &:= \left(af_n+\mathfrak{a}^{n+1}\right)\\ \left(f_n+\mathfrak{a}^{n+1}\right)\left(g_n+\mathfrak{a}^{n+1}\right) &:= \left(\sum_{i+j=n} f_ig_j+\mathfrak{a}^{n+1}\right)\end{aligned}$$

Let us denote $R(\mathfrak{a})_n:=\mathfrak{a}^n/\mathfrak{a}^{n+1}$ where we consider $R(\mathfrak{a})_n$ to be a subset $R(\mathfrak{a})_n\subseteq R(\mathfrak{a})$ canonically (as in (3.30)). We take $R(\mathfrak{a})_n$ to be the *homogeneous* elements of $R(\mathfrak{a})$ of *degree* n. That is we let

$$\big(R(\mathfrak{a})\big)_{\text{hom}} \ :=\ \bigcup_{n\in\mathbb{N}} R(\mathfrak{a})_n\setminus\{0\}$$

Then the Rees-algebra becomes an $\mathbb{N}$-graded $R/\mathfrak{a}$-algebra $(R(\mathfrak{a}),\deg)$ under the following graduation

$$\deg\ :\ \big(R(\mathfrak{a})\big)_{\text{hom}}\to\mathbb{N}\ :\ f_n+\mathfrak{a}^{n+1}\mapsto n$$

Now, if the $\mathfrak{a}$ is a filter-ideal of R and $a\in R$ is a non-zero $a\neq 0$ element of R of order $m:=\operatorname{ord}(a)$, then we can define the **leading form** a^* of a to be the following homogeneous element of degree n. Specifically for $0\in R$ we let $0^*:=(0+\mathfrak{a}^n)\in R(\mathfrak{a})$.

$$a^* \ :=\ \left(a_n+\mathfrak{a}^{n+1}\right) \quad\text{where}\quad a_n\ :=\ \begin{cases} a \text{ if } n=m\\ 0 \text{ if } n\neq m\end{cases}$$

Nota It is obvious that this construction of $R(\mathfrak{a})$ yields an $R/\mathfrak{a}$-module. The next remark (7.44) tells us that $R(\mathfrak{a})$ also is the image of an R-algebra and thereby $R(\mathfrak{a})$ is an R-algebra itself. Together this means that $R(\mathfrak{a})$ is an $R/\mathfrak{a}$-algebra under $(a+\mathfrak{a})(f+\mathfrak{a}^{n+1})=(af+\mathfrak{a}^{n+1})$.

(7.44) Remark: (viz. 788)
Let $(R,+,\cdot)$ be a commutative ring and $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be an ideal of R, then there is an alternate construction of the Rees-algebra: First of all the following set is a sub-algebra of the polynomial ring

$$R_{\mathfrak{a}}[t] \;:=\; \{\, f \in R[t] \mid \forall\, n \in \mathbb{N} : f[n] \in \mathfrak{a}^n \,\}$$

And thereby we find a surjective homomorphism of R algebras from $R_{\mathfrak{a}}[t]$ onto the Rees-algebra $R(\mathfrak{a})$, which is given to be

$$\varrho \;:\; R_{\mathfrak{a}}[t] \twoheadrightarrow R(\mathfrak{a}) \;:\; f \mapsto \left(f[n] + \mathfrak{a}^{n+1}\right)$$

Then the canonical embedding $R \hookrightarrow R[t] : a \mapsto a\mathbf{1}$ takes $\mathfrak{a}$ into $R_{\mathfrak{a}}[t]$. Then the ideal generated by $\{\, a\mathbf{1} \mid a \in \mathfrak{a} \,\} \subseteq R_{\mathfrak{a}}[t]$ is precisely the kernel of this homomorphism

$$\mathrm{kn}(\varrho) \;=\; \mathfrak{a}R_{\mathfrak{a}}[t] \;=\; \left\{\, f \in R[t] \mid \forall\, n \in \mathbb{N} : f[n] \in \mathfrak{a}^{n+} \,\right\}$$

(7.45) Definition:
Let $(D,+)$ and $(E,+)$ be commutative monoids, $(R,+,\cdot)$ be a commutative ring, $(A,\deg)$ be a D-graded and $(B,\deg)$ be an E-graded R-algebra. Then the ordered pair (φ,ε) is said to be a **homomorphism** of **graded algebras** from $(A,\deg)$ to $(B,\deg)$ (or shortly a *graded homomorphism*) iff it satisfies

(1) $\varphi : A \to B$ is a homomorphism of R-algebras

(2) $\varepsilon : D \to E$ is a homomorphism of monoids

(3) $\forall\, h \in A_{\mathrm{hom}}$ we get $\varphi(h) \in B_{\mathrm{hom}}$ and $\deg(\varphi(h)) = \varepsilon(\deg(h))$

If both $(A,\deg)$ and $(B,\deg)$ are D-graded R-algebras, then a homomorphism $\varphi : A \to B$ of R-algebras is said to be **graded** iff $(\varphi,\mathbb{1})$ is a homomorphism of graded algebras, that is iff it satisfies

(1) $\varphi : A \to B$ is a homomorphism of R-algebras

(2) $\forall\, h \in A_{\mathrm{hom}}$ we get $\varphi(h) \in B_{\mathrm{hom}}$

(3) $\forall\, h \in A_{\mathrm{hom}}$ we get $\deg(\varphi(h)) = \deg(h)$

(7.46) Definition: (viz. 783)
Let $(D,+)$ be a commutative monoid, $(R,+,\cdot)$ be a commutative ring and $(A,\deg)$ be a D-graded R-algebra. Then a subset $\mathfrak{h} \subseteq A$ is said to be a **graded ideal** (or *homogeneous ideal*) of $(A,\deg)$, iff $\mathfrak{h} \trianglelefteq_{\mathrm{i}} A$ is an ideal, that satisfies any one of the following three equivalent properties

(a) $\mathfrak{h}$ can be decomposed as the inner direct sum of its R-sub-modules $\mathfrak{h} \cap A_d \leq_{\mathrm{m}} \mathfrak{h}$, that is

$$\mathfrak{h} \;=\; \bigoplus_{d \in D} \mathfrak{h} \cap A_d$$

(b) $\mathfrak{h}$ is closed under going to homogeneous components. That is if $f \in \mathfrak{h}$ is decomposed into homogeneous elements $f = \sum_d f_d$, any homogeneous component $f_d \in A_d$ is an element of $\mathfrak{h}$

$$f = \sum_{d \in D} f_d \in \mathfrak{h} \quad\Longrightarrow\quad \forall\, d \in D : f_d \in \mathfrak{h}$$

(c) $\mathfrak{h}$ is generated (as an ideal) by a set H of homogeneous elements of A, in formal terms that is

$$\exists\, H \subseteq A_{\mathsf{hom}} \quad \text{such that} \quad \mathfrak{h} = \langle H \rangle_{\mathsf{i}}$$

(7.47) Remark:
If $(A, \deg)$ is a D-graded R-algebra and $\mathfrak{a} \trianglelefteq_{\mathsf{i}} A$ is a graded ideal of $(A, \deg)$, then it is clear, that $(\mathfrak{a}, \deg)$ becomes a D-graded R-semi-algebra under the graduation inherited from $(A, \deg)$

$$\begin{aligned} \mathfrak{a}_{\mathsf{hom}} &:= A_{\mathsf{hom}} \cap \mathfrak{a} \\ \deg &:= \deg\big|_{\mathsf{hom}(\mathfrak{a})} \end{aligned}$$

(7.48) Proposition: (viz. 785)
Let $(D, +)$ be a commutative monoid (with neutral element 0), $(R, +, \cdot)$ be a commutative ring and $(A, \deg)$ be a D-graded R-algebra. Then the following statements are true

(i) If D is an integral monoid, then $1 \in A_0$

(ii) If $(B, \deg)$ is another D-graded R-algebra and $\varphi : A \to B$ is a graded homomorphism, then the kernel of φ is a graded ideal in A, therefore we get

$$\mathsf{kn}(\varphi) = \bigoplus_{d \in D} \mathsf{kn}(\varphi) \cap A_d$$

(iii) If $\mathfrak{a} \trianglelefteq_{\mathsf{i}} A$ is a graded ideal of $(A, \deg)$, then the quotient $A/\mathfrak{a}$ becomes a D-graded R-algebra again under the induced graduation $\deg(h + \mathfrak{a}) := \deg(h)$. The homogeneous elements of $A/\mathfrak{a}$ are

$$\left(A \Big/ \mathfrak{a}\right)_{\mathsf{hom}} := \{\, h + \mathfrak{a} \mid h \in A_{\mathsf{hom}} \setminus \mathfrak{a} \,\}$$

And thereby the set of homogeneous elements of degree $d \in D$ is precisely given to be the following

$$\left(A \Big/ \mathfrak{a}\right)_d = A_d + \mathfrak{a} \Big/ \mathfrak{a}$$

(iv) Let $(D, +)$ even be a commutative group and consider a multiplicatively closed subset $U \subseteq A_{\mathsf{hom}}$. Then the localization $U^{-1}A$ (as a ring) is a D-graded R-algebra again. Thereby

$$\left(U^{-1}A\right)_{\mathsf{hom}} := \left\{ \frac{h}{u} \;\middle|\; h \in A_{\mathsf{hom}},\ u \in U \right\} \setminus \left\{ \frac{0}{1} \right\}$$

Then the graduation is defined to be $\deg(h/u) := \deg(h) - \deg(u)$ and the R-sub-module of $U^{-1}R$ of homogeneous elements of any degree $d \in D$ is given to be

$$\left(U^{-1}A\right)_d = \left\{ \frac{h}{u} \;\middle|\; u \in U,\ h \in A_{d+\deg(u)} \right\}$$

(v) Suppose $D = \mathbb{N}$ and consider some ideal $\mathfrak{a} \trianglelefteq_{\mathsf{i}} A$. If now $\mathfrak{a}$ is a graded ideal, then its radical $\sqrt{\mathfrak{a}} \trianglelefteq_{\mathsf{i}} A$ is a graded ideal, too.

(7.49) Remark:
The above statement (iv) has an easy generalization to the case where $(D,+)$ only is an integral, commutative monoid. In this case $U^{-1}A$ becomes a $\mathrm{gr}(D)$-graded R-algebra, where $\mathrm{gr}(D)$ denotes the extension of D to a group, as thereby $\deg(h/u) := \deg(h) - \deg(u) = [\deg(h), \deg(u)]$ is a legit operation in gr (D), again.
Formally that is $\mathrm{gr}(D) := (D \times D)/\sim$ where $(c,d) \sim (c',d') \;:\Longleftrightarrow\; c + d' = c' + d$. Then $\mathrm{gr}(D)$ becomes a well-defined group under $[c,d] + [c',d'] := [c+c', d+d']$ with neutral element $[0,0]$ and $-[c,d] = [d,c]$. And D is included canonically into grD by virtue of $D \hookrightarrow \mathrm{gr}(D) : c \mapsto [c,0]$.

(7.50) Definition:
Let $(R,+,\cdot)$ be a commutative ring, $(D,+,\leq)$ be a positively ordered monoid and $(A,\deg)$ be a D-graded R-algebra. If now $f \in A$ with $f \neq 0$ has the homogeneous decomposition $f = \sum_d f_d$ (where $f_d \in A_d$) then we define

$$\begin{aligned} \deg(f) &:= \max\{\, d \in D \mid f_d \neq 0 \,\} \\ \mathrm{ord}(f) &:= \min\{\, d \in D \mid f_d \neq 0 \,\} \end{aligned}$$

Nota this is well-defined, as only finitely many f_d are non-zero and $\leq$ is a linear order on D. And thus we have defined two functions $\deg : A \setminus \{0\} \to D$ and $\mathrm{ord} : A \setminus \{0\} \to D$ on A.

(7.51) Proposition: (viz. 789)
Let $(R,+,\cdot)$ be a commutative ring, $(D,+,\leq)$ be a positively ordered monoid and $(A,\deg)$ be a D-graded R-algebra. Then the following statements are true

(i) The newly introduced function $\deg : A \setminus \{0\} \to D$ is an extension of the original degree function $\deg : A_{\mathrm{hom}} \to D$. Formally that is

$$h \in A_d,\ h \neq 0 \quad\Longrightarrow\quad \deg(h) = d$$

(ii) It is clear that the *order* and *degree* of some homogeneous element $h \in A_{\mathrm{hom}}$ will agree. But even the converse is true, that is for any non-zero element $f \in \setminus\{0\}$ we get the equivalence

$$f \in A_{\mathrm{hom}} \quad\Longleftrightarrow\quad \mathrm{ord}(f) = \deg(f)$$

(iii) For any elements $f,\ g \in A$ such that $fg \neq 0$ the degree is sub-multiplicative and the order is super-multiplicative. That is we obtain the estimates

$$\begin{aligned} \mathrm{ord}(f) &\leq \deg(f) \\ \deg(fg) &\leq \deg(f) + \deg(g) \\ \mathrm{ord}(fg) &\geq \mathrm{ord}(f) + \mathrm{ord}(g) \end{aligned}$$

(iv) And if $(D, +, \leq)$ is a strictly positively ordered monoid and A is an integral domain, then for any $f, g \in A \setminus \{0\}$ we even get the equalities

$$\begin{aligned} \deg(fg) &= \deg(f) + \deg(g) \\ \operatorname{ord}(fg) &= \operatorname{ord}(f) + \operatorname{ord}(g) \end{aligned}$$

(v) Thus if $(D, +, \leq)$ is a strictly positively ordered monoid and $A \neq 0$ is a non-zero integral domain again, then the invertible elements of A already are homogeneous

$$A^* \subseteq A_{\mathsf{hom}}$$

(vi) If $(D, +, \leq)$ is a strictly positively ordered monoid, A is an integral domain and $h \in A_{\mathsf{hom}}$ is a homogeneous element of A, then any divisor f of h also is a homogeneous element of A, formally

$$f \mid h \implies f \in A_{\mathsf{hom}}$$

7.5 Polynomial Functions

In this section we will be primarily concerned with functions of polynomials f in one variable over a commutative ring R, more specifically with roots of these functions. In case of one variable the sets of solutions of equations of the form $f(x) = 0$, where $f \in R[t]$ is a polynomial, are finite collections of points $x \in R$ only - at least so, if R is an integral domain and $f \neq 0$. In general (with 2 or more variables) this is untrue, e.g. $s - t \in R[s,t]$ already has the solutions (x,x) where $x \in R$. As this is the diagonal in the plane R^2 we already see, that the set of roots of a polynomial in several variables is a geometric object. That is, looking at polynomials, we are able to study both algebra and geometry simultaneously. Yet as $R[s,t]$ is just another version of $R[s][t]$ the restriction to one variable is no restriction at all, for general commutative rings R. It *is* a restriction, when we require the base ring R to be a field, though. Some of the following theorems are veritable cornerstones of algebra and some have direct impact on general polynomial rings $R[t_1,\ldots,t_n]$. As polynomials mimic generic algebraic operations they are the prototype of any algebra. And it is precisely the method of evaluating a polynomial on elements of an R-algebra, that transfers the algebraic operations back into the algebra. This is what makes polynomials so universally useful.

(7.52) Definition:
Let $(R,+,\cdot)$ be a commutative ring and fix any non-empty set $I \neq \emptyset$. Let us also abbreviate the polynomial ring the R-algebra $A := R[t_i \mid i \in I]$ in the variables t_i where i runs over I. That is $A = R[t \mid \mathbb{N}^{\oplus I}]$ is the R-algebra of polynomials over the commutative, integral and solution-finite monoid $\mathbb{N}^{\oplus I}$. No matter what size I has, by definition any $\alpha \in \mathbb{N}^{\oplus I}$ only has finitely many non-zero entries, that is $I(\alpha) := \{\, i \in I \mid \alpha_i \neq 0 \,\}$ is finite. Therefore for *any* I-tuple $x = (x_i) \in R^I$ and any $\alpha = (\alpha_i) \in \mathbb{N}^{\oplus I}$ the following expression yields a well-defined element of R

$$x^\alpha \;:=\; \prod_{i\in I} x_i^{\alpha_i} \;=\; \prod_{i\in I(\alpha)} x_i^{\alpha_i}$$

as the infinite product for $i \in I$ in truth only is a finite product $i \in I(\alpha)$, all the $i \in I \setminus I(\alpha)$ only contribute $x_i^0 = 1$. Likewise for a polynomial $f \in A$ we have required that the set $A(f) := \{\, \alpha \in \mathbb{N}^{\oplus I} \mid f[\alpha] \neq 0 \,\}$ is finite, too. Thus the following expression yields another well-defined element of R

$$f(x) \;:=\; \sum_{\alpha\in\mathbb{N}^{\oplus I}} f[\alpha]\, x^\alpha \;:=\; \sum_{\alpha\in A(f)} f[\alpha]\, x^\alpha$$

Again the seemingly infinite sum over $\alpha \in \mathbb{N}^{\oplus I}$ only runs over the finite subset $A(f)$, all the other $\alpha \in \mathbb{N}^{\oplus I} \setminus A(f)$ only contribute $0 \cdot x^\alpha = 0$. So in the end we find a map of the following form

$$A \times R^I \;\to\; R \;:\; (f,x) \;\mapsto\; f(x)$$

Note that both, $A = R[t_i \mid i \in I]$ and the set of functions $\mathcal{F}(R^I,R) := \{\, f \mid f : R^I \to R \,\}$ are R-algebras. The operations on A have been defined in (7.10.(i)) and the operations on $\mathcal{F}(R^I,R)$ are the point-wise operations $(af)(x) = af(x)$, $(f+g)(x) = f(x) + g(x)$ and $(f\cdot g)(x) = f(x)\cdot g(x)$ respectively.

There's two different ways of turning the above map into a homomorphism of R-algebras: By construction, for any $x \in R^I$ the map $\mathbb{N}^{\oplus I} \to R : \alpha \mapsto x^\alpha$ is a homomorphism of monoids and thereby (7.14) tells us that the following map is a well-defined homomorphism of R-algebras

$$\varepsilon_x \ : \ A \ \to \ R \ : \ f \ \mapsto \ f(x)$$

Thus we have a map $\varepsilon : R^I \to \text{ahom}(A, R) : x \mapsto \varepsilon_x$. This map however does not carry any algebraic structure. On the other hand we can interpret the above map in the following form

$$P \ : \ A \ \to \ \mathcal{F}(R^I, R) \ : \ f \mapsto P_f$$

where $P_f : R^I \to R : x \mapsto f(x)$. This assignment P even is a homomorphism of R-algebras, as $\mathcal{F}(R^I, R)$ is equipped with the pointwise operations. The function P_f is said to be the **polynomial function** induced by $f \in A$. Again it does not carry any algebraic structure. And (by slight abuse of notation) we denote the set of **roots** of P_f by $\mathbb{V}(f)$ again

$$\mathbb{V}(f) \ := \ \mathbb{V}(P_f) \ = \ \left\{ x \in R^I \ \middle| \ f(x) = 0 \right\}$$

(7.53) Remark: $(\diamondsuit)$
This even holds true if $S : R$ is a ring extension and $x = (x_i) \in S^I$. In this case we get $f(x) \in S$ again. That is P_f is a function of the form $P_f : S^n \to S$ and thereby we obtain an homomorphism of R-algebras

$$P \ : \ R[t_i \mid i \in I] \ \to \ \mathcal{F}(S^n, S) \ : \ f \ \mapsto \ P_f$$

As the operations on $\mathcal{F}(S^n, S)$ are point-wise and $P_f(x) = f(x)$ this is to say, that for any $a \in R$, f, $g \in R[t_i \mid i \in I]$ and $x \in S^I$ we have the identities $(af)(x) = af(x)$, $(f+g)(x) = f(x) + g(x)$ and $(f \cdot g)(x) = f(x) \cdot g(x)$. The set of roots of f thereby is a subset of S^I

$$\mathbb{V}_S(f) \ := \ \left\{ x \in S^I \ \middle| \ f(x) = 0 \right\} \ \subseteq \ S^I$$

(7.54) Lemma: (viz. 795)
Let $(R, +, \cdot)$ be a non-zero, commutative ring consider a polynomial $f \in R[t]$ in one variable over R. Let $n := \deg(f)$ be the degree of f, where $\leq$ is the standard total order on $\mathbb{N}$. Then we get

(i) If $a \in R$ is any element of the base ring, $n \in \mathbb{N}$ is any natural number and $g(t) := f(t) \cdot (t - a) \in R[t]$, then we obtain the equivalence of the following two statements

 (a) g is a monic polynomial of degree n

 (b) f is a monic polynomial of degree $n - 1$

(ii) If $f \in R[t]$ is any polynomial over R and $a \in R$ any element of the base ring, then there is another polynomial $q \in R[t]$, such that f can be written in the following form

$$f(t) \ = \ q(t) \cdot (t - a) + f(a)$$

(iii) For any polynomial $f \in R[t]$ and any $a \in R$ we find, that the evaluation $f(a) = 0$ is zero, if and only if the polynomial $t - a$ divides f in $R[t]$. Formally this is the equivalence

$$f(a) \;=\; 0 \quad\Longleftrightarrow\quad (t-a) \;\mid\; f(t)$$

(iv) If R is an integral domain and $x_1, \ldots, x_m$ are pairwise distinct roots of f [that is for all $i, j \in 1 \ldots m$ we have $f(x_i) = 0$ and $x_i = x_j \implies i = j$] then there is some polynomial $q \in R[t]$ such that

$$f(t) \;=\; (t - x_1) \ldots (t - x_m)\, q(t)$$

In particular, if R is an integral domain and $f \neq 0$ is non-zero, then the number of distinct roots of f cannot exceed the degree of f. In formal terms that is

$$\#\{\, x \in R \mid f(x) = 0 \,\} \;\leq\; \deg(f)$$

(v) If R is an integral domain and $f, g \in R[t]$ are polynomials, whose number of intersection points exceed their degrees, then f and g already are equal. Formally that is

$$\max\{\, \deg(f), \deg(g) \,\} \;<\; \#\{\, x \in R \mid f(x) = g(x) \,\} \quad\Longrightarrow\quad f \;=\; g$$

(7.55) Example:
If R is not an integral domain, then the equation $f(x) = 0$, where $f \in R[t]$ can have more solutions, than $n = \deg(f)$. As an example consider $R = \mathbb{Z}_8$ and $f(t) := t^2 - 1$. In this case $f(x) = 0$ boasts 4 different solutions, namely

$$\{\, x \in \mathbb{Z}_8 \mid x^2 - 1 \,\} \;=\; \{\, 1, 3, 5, 7 \,\}$$

This example also shows, that (in a non-integral domain) $x^2 = 1$ can have more solutions than the classical 1 and -1. And in fact these roots give rise to two distinct factorisations of f, namely

$$t^2 - 1 \;=\; (t-1)(t-7) \;=\; (t-3)(t-5)$$

(7.56) Example: (viz. 797)
Let $(R, +, \cdot)$ be a commutative ring, $1 \leq n \in \mathbb{N}$ and let us abbreviate $S := R[t_1, \ldots, t_n]$ and the n-tuple $t := (t_1, \ldots, t_n) \in S^n$. If now $A = (a_{i,j}) \in \mathrm{mat}_n(R)$ is a square matrix, then we define the following R-algebra-endomorphism on S, by linear expansion of

$$\varphi_A \;:\; S \to S \;:\; t_i \mapsto [At]_i \;=\; \sum_{j=1}^{n} a_{i,j} t_j$$

That is φ_A is the uniquely determined R-algebra-homomorphism, that satisfies $\varphi_A(t_i) = [At]_i$ which exists by (7.14). Then we clearly have (i) if $E = \mathbb{1}_n$ is the identity matrix, then $\varphi_E = \mathbb{1}_S$ and (ii) if $B \in \mathrm{mat}_n(R)$ is any other $(n \times n)$-matrix, then $\varphi_B\, \varphi_A = \varphi_{AB}$. In particular (iii) if A is invertible, then φ_A is an R-algebra-automorphism of S with inverse $\varphi_{A^{-1}}$.

(7.57) Proposition: (viz. 798)
Let $(F,+,\cdot)$ be a field $1 \leq n \in \mathbb{N}$ and consider the polynomial ring in n variables $F[t_1,\ldots,t_n]$. Also let $f \in F[t_1,\ldots,t_n]$ be a non-zero polynomial $f \neq 0$. Let x_1 to x_n be the variable symbols of another polynomial ring $F[x_1,\ldots,x_n]$ and denote $R := F[x_2,\ldots,x_n]$. Then we find the following coordinate transforms to which f can be subjected

(i) If F is infinite (actually it suffices, that F is an infinite integral domain) and f is homogeneous, then there are some $a_2,\ldots,a_n \in F$ such that

$$f(1,a_2,\ldots,a_n) \quad \neq \quad 0 \quad \in \quad F$$

(ii) If F is infinite (and a field), then there are scalars $a \in F$ and $a_2,\ldots,a_n \in F$ such that the following polynomial in the variables x_1 to x_n is monic, if written as a polynomial in x_1 over R:

$$af\big(x_1, x_2 + a_2x_1, \ldots, x_n + a_nx_1\big) \quad \in \quad R[x_1]$$

(iii) For any field F there are some $a \in F$ and numbers $1 \leq m_2,\ldots,m_n \in \mathbb{N}$ such that the following polynomial in the variables x_1 to x_n is monic, if written as a polynomial in x_1 over R:

$$af\big(x_1, x_2 + x_1^{m_2}, \ldots, x_n + x_1^{m_n}\big) \quad \in \quad R[x_1]$$

(7.58) Remark: (viz. 799) **Interpolation**
Consider an integral domain $(R,+,\cdot)$ and some points $(x_i,y_i) \in R^2$ in the plane of R, where $1 \leq n \in \mathbb{N}$. To avoid redundancies or contradictions we have to assume that the x_i are pairwise distinct [i.e. $x_i = x_j$ implies $i = j$]. We are looking for a polynomial $f \in R[t]$ that satisfies $f(x_i) = y_i$ for any $i \in 1\ldots n$. As we have n unknown $y_1,\ldots,y_n \in R$ it stands to reason to also regard n variables - the coefficients of f

$$f(t) \quad = \quad f[n-1]t^{n-1} + \cdots + f[1]t + f[0]$$

(i) *Brute Force*: The set $\mathcal{P}_n := \{\, f \in R[t] \mid \deg(f) < n \,\}$ is a free R-module of dimension n, as a basis is given to be $\{\, \mathbf{1}, t, \ldots, t^{n-1} \,\}$. If we write out $f(x_i) = y_i$ we arrive at $f[n-1]x_i^{n-1} + \cdots + f[1]x_i + f[0] = y_i$. As this shall be true for any $i \in 1\ldots n$ we arrive at an $n \times n$-system of linear equations

$$\begin{pmatrix} 1 & x_1 & \cdots & x_1^{n-1} \\ 1 & x_2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & x_n & \cdots & x_n^{n-1} \end{pmatrix} \begin{pmatrix} f[0] \\ f[1] \\ \vdots \\ f[n-1] \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$$

The $n \times n$-matrix occurring in this system is called the *Vandermonde* matrix of the x_i, denoted by $\mathrm{Van}(x_1,\ldots,x_n)$. By Laplace-expansion of the determinant we find that the determinant of this matrix is given to be the product of the $x_j - x_i$ where $i < j$:

$$\det\Big(\mathrm{Van}(x_1,\ldots,x_n)\Big) \quad = \quad \prod_{1 \leq i < j \leq n} (x_j - x_i)$$

Hence, if this determinant is a unit of R, we may compute the coefficients of f by solving this

system of linear equations. In effect we get: If the determinant of the Vandermonde matrix of the x_i, is a unit of R, then there is a uniquely determined polynomial f of degree $\deg(f) < n$ such that $f(x_i) = y_i$ for all $i \in 1 \ldots n$. While this is feasible in theory this approach is rarely used for practical computations, as solving this system takes too much effort.

(ii) *Lagrange Interpolation*: We use that $\mathcal{P}_n := \{ f \in R[t] \mid \deg(f) < n \}$ is a free R-module of dimension n again, but this time we choose a more suitable basis: For a fixed $j \in 1 \ldots n$ let

$$\ell_j(t) \;:=\; \prod_{i \neq j} (t - x_i)$$

which is a polynomial of degree $n-1$ over R. Let $u_j := \ell_j(x_j)$ and suppose that all the $u_j \in R^*$ are invertible. Then we may introduce the following polynomials

$$L_j(t) \;:=\; u_j^{-1}\, \ell_j(t) \;=\; \prod_{i \neq j} \frac{t - x_i}{x_j - x_i}$$

Then by construction we have $L_j(x_i) = \delta_{i,j}$ and hence $\{ L_1, \ldots, L_n \} \subseteq \mathcal{P}_n$ is a linearly independent subset, even a basis of $\mathcal{P}_n$. And we obtain a polynomial $f \in \mathcal{P}_n$ such that $f(x_i) = y_i$ (for any $i \in 1 \ldots n$) simply by taking

$$f(t) \;:=\; \sum_{i=1}^{n} y_i\, L_i(t)$$

(iii) *Newtonian Interpolation*: Lies somewhere in between the brute force approach and the approach of Lagrange. Again we try to find $f \in \mathcal{P}_n$ as a linear combination of certain polynomials $N_j \in \mathcal{P}_n$

$$f(t) \;=\; \sum_{j=0}^{n-1} a_j\, N_j(t)$$

However in this case we start with $N_0(t) := \mathbf{1}$ and for $j \in 1 \ldots n-1$ we recursively define N_j by

$$N_j(t) \;:=\; N_{j-1}(t) \cdot (t - x_j) \;=\; \prod_{i=1}^{j} (t - x_i)$$

In particular we have $\deg(N_j) = j$ and thereby $N_j \in \mathcal{P}_n$. Also for any $i \in 1 \ldots j$ we see that $N_j(x_i) = 0$ by construction. Hence for any $i \in 1 \ldots n$ the equation $f(x_i) = y_i$ is reduced to the sum of $a_j N_j(x_i)$ where $j < i < n$. In the language of matrices that is

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & N_1(x_2) & 0 & \cdots & 0 \\ 1 & N_1(x_3) & N_2(x_3) & & \\ \vdots & \vdots & \vdots & \ddots & \\ 1 & N_1(x_n) & N_2(x_n) & \cdots & N_{n-1}(x_n) \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} \;=\; \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$$

This SLE can be solved if for any $i \in 2 \dots n$ we have $N_{i-1}(x_i) \in R^*$ is a unit. Thereby the product of the $N_{i-1}(x_i)$ is the determinant of the Vandermonde matrix, hence this again is equivalent to the determinant being invertible. The advantage of this approach is (1) this SLE is easy to solve, (2) the polynomials $N_j(t)$ can be computed recursively and (3) it is easy to append another point (x_{n+1}, y_{n+1}) by just adding another row to the matrix. This makes this method the preferred algorithm for interpolation in numerical applications.

(7.59) Corollary: (viz. 801)

(i) Let $(F, +, \cdot)$ be a field, $1 \leq n \in \mathbb{N}$ and consider $(x_i, y_i) \in F^2$ such that $x_i = x_j$ implies $i = j$. Then there is a uniquely determined polynomial $f \in F[t]$ that satisfies the following two properties

(1) $\deg(f) < n$

(2) $\forall\, i \in 1 \dots n$ we get $f(x_i) = y_i$

(ii) Let $(F, +, \cdot)$ be a field and consider the map $P : F[t] \to \mathcal{F}(F, F)$ given by $P : f \mapsto P_f$ where $P_f : F \to F : x \mapsto f(x)$. If F is finite then P is surjective, but not injective. And if F is infinite then P is injective but not surjective. Formally

$$\begin{aligned} \#F &< \infty \iff f \mapsto P_f \text{ is surjective} \\ \#F &= \infty \iff f \mapsto P_f \text{ is injective} \end{aligned}$$

Algebraic Sets:
So far for polynomials in one variable only. Let us take a very short glance behind the curtain: Algebraic Geometry studies the set of roots of a polynomial in severable variables in case the base ring R is an algebraically closed field. Though this would be a course of its own, let us introduce the basic notions here, up to the Zariski-topology on the space R^I:
So what is a root, anyway? Recall that if $f \in R[t_i \mid i \in I]$ is a polynomial over a commutative ring R and S is a commutative R-algebra and $x = (x_i) \in S^I$ is a point we have defined in (7.52)

$$f(x) \;:=\; \sum_{\alpha \in \mathbb{N}^{\oplus I}} f[\alpha] \prod_{i \in I} x_i^{\alpha_i}$$

And thereby $R[t_i \mid i \in I] \to S : f \mapsto f(x)$ is a homomorphism of R-algebras according to (7.14). If $f(x) = 0$ we say that x is a **root** of f or equivalently that x **satisfies** f. So where's the geometry? Here it is: E.g. in three dimensional space, the following equation defines a sphere of radius r around the centre $C = (c_1, c_2, c_3) \in R^3$

$$f(t_1, t_2, t_3) \;:=\; (t_1 - c_1)^2 + (t_2 - c_2)^2 + (t_3 - c_3)^2 - r^2$$

The set of $x \in R^3$ that satisfy f (that is $f(x) = 0$) geometrically has the shape of this sphere. Generally speaking geometric objects are sets of roots of functions and combinations thereof. In algebraic geometry these equations are taken to be polynomial and this already allows a multitude of objects.

So what do we mean by combinations thereof? If $X \subseteq S^I$ is defined by the equation $f \in R[t_i \mid i \in I]$ and likewise $Y \in R^I$ is defined by $g \in R[t_i \mid i \in I]$ then the intersection $X \cap Y$ is defined by $f(x) = 0$ *and* $g(x) = 0$. Likewise the union $X \cup Y$ is defined by $f(x) = 0$ *or* $g(x) = 0$. If S is an integral domain, this is $(f \cdot g)(x) = 0$. Here we already see that geometric operations correspond to algebraic compositions. Let us dig just a little deeper:

(7.60) Definition:
Let $(R, +, \cdot)$ be a commutative ring and fix any non-empty index set I. If $F \subseteq R[t_i \mid i \in I]$ respectively $X \subseteq R^I$ are arbitrary subsets, then we define the **algebraic set** to be the common zero-locus $\mathbb{V}(F)$ of the polynomials $f \in F$, respectively the **vanishing ideal** $\mathbb{I}(X)$ to be the set of polynomials that vanish on X identically. Formally that is

$$\begin{aligned} \mathbb{V}(F) &:= \left\{ x \in R^I \;\middle|\; \forall f \in F : f(x) = 0 \right\} \\ \mathbb{I}(X) &:= \{ f \in R[t_i \mid i \in I] \mid \forall x \in X : f(x) = 0 \} \end{aligned}$$

Nota If $f \in R[t_i \mid i \in I]$ is a single polynomial, then (by slight abuse of notation) we abbreviate $\mathbb{V}(f) := \mathbb{V}(\{ f \}) = \{ x \in R^I \mid f(x) = 0 \}$ the algebraic set of f. And likewise, for a single point $x \in R^I$ we abbreviate $\mathbb{I}(x) := \mathbb{I}(\{ x \}) = \{ f \in R[t_i \mid i \in I] \mid f(x) = 0 \}$ the vanishing ideal of x.

(7.61) Proposition: (viz. 802)
Let $(R, +, \cdot)$ be a commutative ring and fix any non-empty index set I. Then we find the following relations between the algebraic sets $\mathbb{V}(F)$ and vanishing ideals $\mathbb{I}(X)$:

(i) Let $f \in R[t_i \mid i \in I]$ be a polynomial and $X \subseteq R^I$ be an arbitrary subset. Then from the above definitions it is immediately clear, that we have the following equivalences

$$f \in \mathbb{I}(X) \iff X \subseteq \mathbb{V}(f) \iff \mathbb{V}\mathbb{I}(X) \subseteq \mathbb{V}(f)$$

Likewise, if $F \subseteq R[t_i \mid i \in I]$ is any family of polynomials over R and $x \in R^I$ is any point, then we similarly obtain the following equivalences

$$x \in \mathbb{V}(F) \iff F \subseteq \mathbb{I}(x) \iff \mathbb{I}\mathbb{V}(F) \subseteq \mathbb{I}(x)$$

(ii) Let $X \subseteq R^I$ be an arbitrary subset, then the vanishing ideal $\mathbb{I}(X)$ of X truly is an ideal of $R[t_i \mid i \in I]$. And if $\text{NIL}(R) = 0$, then $\mathbb{I}(X)$ even is a radical ideal. Formally that is

$$\sqrt{\mathbb{I}(X)} = \mathbb{I}(X) \trianglelefteq_{\mathrm{i}} R[t_i \mid i \in I]$$

(iii) Let $F \subseteq R[t_i \mid i \in I]$ be an arbitrary subset and let $\mathfrak{a} := \langle F \rangle_{\mathrm{i}}$ denote the ideal of $R[t_i \mid i \in I]$ generated by F. Then F defines the same algebraic set as $\mathfrak{a}$ itself (that is $\mathbb{V}(F) = \mathbb{V}(\mathfrak{a})$) and if $\text{NIL}(R) = 0$, then we even get

$$\mathbb{V}(F) = \mathbb{V}(\mathfrak{a}) = \mathbb{V}(\sqrt{\mathfrak{a}})$$

(iv) For the moment being let us denote $A := R[t_i \mid i \in I]$ the R-algebra of the polynomial ring and the power sets, its set of ideals $\mathrm{Ideal}(A) := \{\mathfrak{a} \mid \mathfrak{a} \trianglelefteq_{\mathrm{i}} A\}$ and the power set $\mathcal{P}(R^I) := \{X \mid X \subseteq R^I\}$ of R^I. Then we have the defined the functions

$$\begin{aligned} \mathbb{V} &: \mathrm{Ideal}(A) \to \mathcal{P}(R^n) &&: \mathfrak{a} \mapsto \mathbb{V}(\mathfrak{a}) \\ \mathbb{I} &: \mathcal{P}(R^n) \to \mathrm{Ideal}(A) &&: X \mapsto \mathbb{I}(X) \end{aligned}$$

Note that both, the power set $\mathcal{P}(R^I)$ and the set $\mathrm{Ideal}(A)$ of ideals, are partially ordered under the inclusion "$\subseteq$" of sets. Then we find that $\mathbb{V}$ and $\mathbb{I}$ form a *Galois connection* between these ordered sets. That is for any $X, Y \subseteq R^I$ and any $\mathfrak{a}, \mathfrak{b} \trianglelefteq_{\mathrm{i}} R[t_i \mid i \in I]$ we get

$$\begin{aligned} X \subseteq Y &\implies \mathbb{I}(X) \subseteq \mathbb{I}(Y) \\ \mathfrak{a} \subseteq \mathfrak{b} &\implies \mathbb{V}(\mathfrak{b}) \subseteq \mathbb{V}(\mathfrak{a}) \\ X &\subseteq \mathbb{V}\mathbb{I}(X) \\ \mathfrak{a} &\subseteq \mathbb{I}\mathbb{V}(\mathfrak{a}) \end{aligned}$$

In particular by (0.22) we have $\mathbb{V}\mathbb{I}\mathbb{V} = \mathbb{V}$ and $\mathbb{I}\mathbb{V}\mathbb{I} = \mathbb{I}$. And thereby $\mathbb{V}$ and $\mathbb{I}$ are bijective, mutually inverse maps when restricted to the respective images, that is a 1-to-1 correspondence

$$\begin{aligned} \mathbb{V}\big(\mathrm{Ideal}(A)\big) &\longleftrightarrow \mathbb{I}\big(\mathcal{P}(R^I)\big) \\ X &\mapsto \mathbb{I}(X) \\ \mathbb{V}(\mathfrak{a}) &\hookleftarrow \mathfrak{a} \end{aligned}$$

(v) Consider the non-empty index sets $\Lambda = 1 \ldots n$ or an arbitrary $\Lambda \neq \emptyset$ respectively. For any $\lambda \in \Lambda$ let $\mathfrak{a}_\lambda \trianglelefteq_{\mathrm{i}} R[t_i \mid i \in I]$ be an ideal. Then the respective algebraic sets satisfy the properties

$$\begin{aligned} \mathbb{V}(0) &= R^I \\ \mathbb{V}(\mathfrak{a}_1) \cup \cdots \cup \mathbb{V}(\mathfrak{a}_n) &\subseteq \mathbb{V}\big(\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n\big) \\ \mathbb{V}\big(\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n\big) &\subseteq \mathbb{V}\big(\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n\big) \\ \mathbb{V}\left(\sum_{\lambda\in\Lambda} \mathfrak{a}_\lambda\right) &= \bigcap_{\lambda\in\Lambda} \mathbb{V}(\mathfrak{a}_\lambda) \end{aligned}$$

And if R is an integral domain we even get $\mathbb{V}(\mathfrak{a}_1) \cup \cdots \cup \mathbb{V}(\mathfrak{a}_n) = \mathbb{V}(\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n) = \mathbb{V}(\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n)$. Conversely let $X_\lambda \subseteq R^I$ be arbitrary subsets of the I-dimensional space over R (where $\lambda \in \Lambda$), then we retain some of the dual properties of the above, that is we also have

$$\begin{aligned} \mathbb{I}(\emptyset) &= R[t_i \mid i \in I] \\ \bigcap_{\lambda\in\Lambda} \mathbb{I}(X_\lambda) &= \mathbb{I}\left(\bigcup_{i\in I} X_i\right) \\ \sum_{\lambda\in\Lambda} \mathbb{I}(X_\lambda) &\subseteq \mathbb{I}\left(\bigcap_{\lambda\in\Lambda} X_\lambda\right) \end{aligned}$$

(vi) If $R \neq 0$ is non-zero, then $\mathbb{V}(R[t_i \mid i \in I]) = \emptyset$. And if R is an infinite integral domain (i.e. $\#R = \infty$), then the vanishing ideal of the entire space R^I is the zero-ideal, formally

$$\mathbb{I}(R^I) \;=\; 0$$

(7.62) Remark: (viz. 804)
If $(R, +, \cdot)$ is an integral domain, then we have just seen, that the algebraic sets $\mathbb{V}(\mathfrak{a})$ are closed under finite unions and arbitrary intersections, as we have the identities

$$\begin{aligned} \mathbb{V}(\mathfrak{a}_1) \cup \cdots \cup \mathbb{V}(\mathfrak{a}_n) &= \mathbb{V}\big(\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n\big) \\ \bigcap_{i \in I} \mathbb{V}(\mathfrak{a}_i) &= \mathbb{V}\left(\sum_{i \in I} \mathfrak{a}_i\right) \end{aligned}$$

As also $\mathbb{V}(0) = R^n$ and $\mathbb{V}(R[t_i \mid i \in I]) = \emptyset$ the algebraic sets form the *closed* sets of a topology on R^I. This is called the *Zariski topology* of R^I and this is the staging area of algebraic geometry

$$\mathcal{Z}\big(R^I\big) \;:=\; \{\, \mathbb{V}(\mathfrak{a}) \mid \mathfrak{a} \trianglelefteq_{\mathrm{i}} R[t_1, \ldots, t_n] \,\}$$

Conversely let $\mathcal{I}(R^I) := \{\mathbb{I}(X) \mid X \subseteq R^I\}$ be the set of ideals of $R[t_i \mid i \in I]$ that occur as vanishing ideals of subsets $X \subseteq R^I$. Then we know by (7.61.(ii)), that $\mathcal{I}(R^I) \subseteq \mathrm{Srad}(R[t_i \mid i \in I])$. And by (7.61.(iv)) the Galois connection of $\mathbb{I}$ and $\mathbb{V}$ restricts to the following 1-to-1 correspondence

$$\begin{aligned} \mathcal{Z}\big(R^I\big) &\longleftrightarrow \mathcal{I}\big(R^I\big) \\ X &\mapsto \mathbb{I}(X) \\ \mathbb{V}(\mathfrak{a}) &\hookleftarrow \mathfrak{a} \end{aligned}$$

The question, whether any radical ideal of $R[t_i \mid i \in I]$ occurs as a vanishing ideal of some algebraic set will be answered by Hilbert's Nullstellensatz in section 8.5: This will only be the case, for algebraically closed fields R. Even for the field of real numbers $R = \mathbb{R}$, the maximal ideal $\mathfrak{z} := (t^2 + 1)\mathbb{R}[t]$ satisfies $\mathbb{V}(\mathfrak{z}) = \emptyset$ and hence $\mathfrak{z} \subset \mathbb{R}[t] = \mathbb{I}\mathbb{V}(\mathfrak{z})$. That is $\mathfrak{z}$ is not a vanishing ideal of an algebraic set. However for an integral domain we get

(i) For any subset $X \subseteq R^I$ the closure of X in the Zariski-topology is given to be $\overline{X} = \mathbb{V}\mathbb{I}(X)$.

(ii) If R infinite and $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R[t_i \mid i \in I]$ is any ideal, then we have $\mathbb{V}(\mathfrak{a}) = R^I$ if and only if $\mathfrak{a} = 0$.

Symmetric Polynomials:
After this excursion into the set of roots of polynomials in arbitrarily many variables, let us return to the case of one variable only. This is not a real restriction, as we can shove off all but one variable down into the base ring, using the isomorphy of $R[t_1, \ldots, t_n]$ and $R[t_2, \ldots, t_n][t_1]$. So we still are interested in the roots of a polynomial in one variable, but this time we take take the back door: What if we knew all the roots, what can we say about its coefficients, then?

The answer to this question is provided by the theorem of Vieta. In order to formulate this we have to introduce symmetric polynomials, which are of interest in their own right. We begin with an example, that illustrates how the elementary symmetric polynomials emerge. After this we will formulate prove the theorem of Vieta - even though the polynomial in question has a single variable only, it has several roots. And as we represent any root by a variable, symmetric polynomials have finitely many variables, by nature. We conclude by studying symmetric polynomials in general.

(7.63) Example:
Consider any commutative ring R, e.g. $R = \mathbb{Z}$ and a monic polynomial $f \in R[t]$. We are interested in the *roots* of f, that is the solutions $x \in R$ to the equation $f(x) = 0$. As these can be very hard to find, let us first start the other way round: Suppose that f *splits* over R, that is there are some $x_1, \ldots, x_n \in R$ such that f can be written, as

$$f(t) \;=\; (t - x_1)(t - x_2) \ldots (t - x_n)$$

Then clearly for any $i \in 1 \ldots n$ we have $f(x_i) = 0$ and (if R is an integral domain), these also are the only solutions to $f(x) = 0$. So how do the roots build up the coefficients of f? In case $n = 1$ we see $f[1] = 1$ and $f[0] = -x_1$. This is not very instructive. In case $n = 2$ we compute

$$f(t) \;=\; t^2 - (x_1 + x_2)t + x_1x_2$$

That is $f[1]$ is the negative sum of the roots, whereas $f[0]$ is the product of the roots. Let us check, what happens in case $n = 3$, here we find

$$f(t) \;=\; t^3 - (x_1 + x_2 + x_3)t^2 + (x_1x_2 + x_1x_3 + x_2x_3)t - x_1x_2x_3$$

Again the second highest coefficient $f[2]$ is the negative sum of the roots, and the constant term $f[0]$ is the negative product of the roots - it seems we are after something (the theorem of Vieta). The middle coefficient $f[1]$ is a little weird, at first glance. But it a sum of pairs x_ix_j. No wonder: $f[k]$ is accompanied by t^k so we need to pick $n - k$ of the x_i from the brackets, when expanding the term of f. Thereby any combination of x_i is allowed, but of course we may not pick from the same bracket twice. This is the reasoning behind the definition of the elementary symmetric polynomials (see below) and the reason why the theorem of Vieta holds true.

(7.64) Definition:
For any $1 \leq n \in \mathbb{N}$ denote $S_n := \{\, \sigma : 1 \ldots n \to 1 \ldots n \mid \sigma \text{ is bijective} \,\}$ the set of permutations again. Also let $(R, +, \cdot)$ be any ring and $f \in R[t_1, \ldots, t_n]$ be a polynomial in n variables over R. If $\sigma \in S_n$ is any permutation, we denote

$$\sigma f \;:=\; f\big(t_{\sigma(1)}, \ldots, t_{\sigma(n)}\big) \;=\; \sum_{\alpha \in \mathbb{N}^n} f[\alpha]\, t_{\sigma(1)}^{\alpha_1} \ldots t_{\sigma(n)}^{\alpha_n} \;\in\; R[t_1, \ldots, t_n]$$

Now a polynomial $f \in R[t_1,\dots,t_n]$ is said to be **symmetric** iff it is invariant under any permutation. That is iff for any $\sigma \in S$ we see $\sigma f = f$. We denote the set of all symmetric polynomials by

$$R[t_1,\dots,t_n]_{\text{sym}} \;:=\; \{\, f \in R[t_1,\dots,t_n] \mid \forall\, \sigma \in S_n \,:\, \sigma f = f \,\}$$

And a polynomial $f \in R[t_1,\dots,t_n]$ is said to be **anti-symmetric** iff its sign changes under permutation. That is iff for any $\sigma \in S$ we see $\sigma f = \operatorname{sgn}(\sigma) f$. We denote the set of all anti-symmetric polynomials by

$$R[t_1,\dots,t_n]_{\text{asym}} \;:=\; \{\, f \in R[t_1,\dots,t_n] \mid \forall\, \sigma \in S_n \,:\, \sigma f = \operatorname{sgn}(\sigma) f \,\}$$

Recall that for $k \in 1\dots n$ we defined $\operatorname{Asc}(k,n) = \{\, \alpha : 1\dots r \to 1\dots n \mid \alpha(1) < \alpha(2) < \cdots < \alpha(k) \,\}$ the set of k ascending indices in $1\dots n$. We use this to introduce the k-th **elementary symmetric** polynomial in n variables to be the following polynomial of $R[t_1,\dots,t_n]$:

$$s_k^{(n)}(t_1,\dots,t_n) \;:=\; \sum_{\alpha \in \operatorname{Asc}(k,n)} t_{\alpha(1)} \dots t_{\alpha(k)}$$

Nota for ease of notation it is sometimes beneficial to also take $s_0^{(n)}(t_1,\dots,t_n) := 1$. And by definition it is clear, that $s_1^{(n)}(t_1,\dots,t_n) = t_1 + t_2 + \cdots + t_n$ up to $s_n^{(n)}(t_1,\dots,t_n) = t_1 t_2 \dots t_n$. For ease of understanding let us also write out $s_2^{(n)}(t_1,\dots,t_n)$ in more informal terms

$$s_2^{(n)}(t_1,\dots,t_n) \;=\; t_1t_2 + t_1t_3 + \cdots + t_1t_n + t_2t_3 + t_2t_4 + \cdots + t_{n-1}t_n$$

(7.65) Remark:
Clearly $S_n \times R[t_1,\dots,t_n] \to R[t_1,\dots,t_n] : (\sigma, f) \mapsto \sigma f$ is a group action. That is for any polynomial $f \in R[t_1,\dots,t_n]$ and any permutations $\varrho, \sigma \in S_n$ we have the properties

$$\mathbb{1}_n f \;=\; f \quad \text{and} \quad \sigma\big(\varrho f\big) \;=\; \big(\sigma\varrho\big) f$$

And thereby for a fixed permutation $\sigma \in S_n$ the map $T_\sigma(f) := \sigma f$ is an R-algebra automorphism of $R[t_1,\dots,t_n]$, with inverse $(T_\sigma)^{-1} = T_{\sigma^{-1}}$. That is we have $\sigma\mathbf{0} = \mathbf{0}$, $\sigma\mathbf{1} = \mathbf{1}$ and for any scalar $a \in R$ and polynomials $f, g \in R[t_1,\dots,t_n]$ also

$$\begin{aligned} \sigma(af) &= a\,(\sigma f) \\ \sigma(f+g) &= (\sigma f) + (\sigma g) \\ \sigma(f\cdot g) &= (\sigma f)\cdot(\sigma g) \end{aligned}$$

Prob the properties of a group action are immediately clear from the definition and $(T_\sigma)^{-1} = T_{\sigma^{-1}}$ is consequential. The properties of an R-algebra homomorphism are covered by (7.14), as σf has been defined by the evaluation $f(t_{\sigma(1)},\dots,t_{\sigma(n)})$.

(7.66) Theorem: (viz. 804)
Let $(R,+,\cdot)$ be a commutative ring and fix some $1 \leq n \in \mathbb{N}$. First of all recall the usual degree $\deg(f)$ and weight $\mathrm{wgt}(f)$ of a polynomial $f \in R[t_1,\ldots,t_n]$ in n variables

$$\begin{aligned}\deg(f) &:= \max\{\,\alpha_1+\cdots+\alpha_n \mid \alpha \in \mathbb{N} \text{ and } f[\alpha] \neq 0\,\}\\ \mathrm{wgt}(f) &:= \max\{\,1\cdot\alpha_1+\cdots+n\cdot\alpha_n \mid \alpha \in \mathbb{N} \text{ and } f[\alpha] \neq 0\,\}\end{aligned}$$

(i) For any $k \in 1\ldots n$ the k-th elementary symmetric polynomial $s_k^{(n)}$ in n variables is of degree k. And for any polynomial $f \in R[t_1,\ldots,t_n]$ we find the following identity

$$\begin{aligned}\deg\big(s_k^{(n)}\big) &= k\\ \deg\big(f(s_1^{(n)},\ldots,s_n^{(n)})\big) &= \mathrm{wgt}(f)\end{aligned}$$

(ii) For $k=0$ we have $s_0^{(n)}=1$ and for $n \geq 2$ and $k \geq 1$ the elementary symmetric polynomials in n variables can be generated by recursion on elementary symmetric polynomials in $n-1$ variables:

$$s_k^{(n-1)} + s_{k-1}^{(n-1)}\, t_n = s_k^{(n)}$$

(iii) *Theorem of Vieta*: For any n-tuple $a=(a_1,\ldots,a_n) \in R^n$ of scalars, the product $(t-a_1)\ldots(t-a_n)$ is a polynomial of degree n over R, whose coefficients are the elementary symmetric polynomials evaluated in a, formally we find

$$\prod_{k=1}^{n}(t-a_k) = t^n + \sum_{k=0}^{n-1}(-1)^{n-k}\, s_{n-k}^{(n)}(a)\, t^k$$

In other words: If $f \in R[t]$ splits over R, then we can express its coefficients in terms of the elementary symmetric polynomials in its roots: That is if $f(t)=b(t-a_1)\ldots(t-a_n)$ then for any $k \in 0\ldots n$ the k-th coefficient of f is given to be

$$f[k] = (-1)^{n-k}\, b\, s_{n-k}^{(n)}(a_1,\ldots,a_n)$$

(7.67) Proposition: (viz. 805)
Let $(R,+,\cdot)$ be a commutative ring and regard the polynomial ring $R[t_1,\ldots,t_n]$ in $1 \leq n \in \mathbb{N}$ variables over R. We abbreviate the elementary symmetric polynomials by $s_k := s_k^{(n)} \in R[t_1,\ldots,t_n]$. Then the following statements are true

(i) The symmetric polynomials form an R-subalgebra of $R[t_1,\ldots,t_n]$ and this subalgebra is generated by the elementary symmetric polynomials, formally that is

$$R[t_1,\ldots,t_n]_{\mathrm{sym}} = R[s_1,\ldots,s_n] = \{\, f(s_1,\ldots,s_n) \mid f \in R[t_1,\ldots,t_n]\,\}$$

(ii) Let $f \in R[t_1,\ldots,t_n]$ be any polynomial and regard f in the isomorphic copy $R[t_1,\ldots,t_{n-1}][t_n]$ of $R[t_1,\ldots,t_n]$. That is we write f in the form

$$f = f[0] + f[1]\, t_n + \cdots + f[d]\, t_n^d \quad \text{where} \quad f[k] \in R[t_1,\ldots,t_{n-1}]$$

Now, if f is symmetric, then for any $k \in \mathbb{N}$ the coefficient polynomial $f[k]$ of f is a symmetric polynomial in $R[t_1, \ldots, t_{n-1}]$, as well. That is we get the implication

$$f \text{ is symmetric} \quad \Longrightarrow \quad \forall\, k \in \mathbb{N} \;:\; f[k] \text{ is symmetric}$$

(iii) The evaluation of a polynomial in the elementary symmetric polynomials is injective. That is: For any two polynomials $f, g \in R[t_1, \ldots, t_n]$ we obtain the equivalence

$$f(s_1, \ldots, s_n) \;=\; g(s_1, \ldots, s_n) \quad \Longleftrightarrow \quad f \;=\; g$$

In particular any symmetric polynomial $s \in R[t_1, \ldots, t_n]$ can be expressed uniquely in terms of the elementary symmetric polynomials. And this polynomial g generating s satisfies $\mathrm{wgt}(g) \leq \deg(s)$.

$$\exists!\, g \in R[t_1, \ldots, t_n] \quad \text{such that} \quad s \;=\; g(s_1, \ldots, s_n)$$

(iv) $(\diamondsuit)$ Let $S : R$ be a ring extension and $f \in R[t]$ be a monic polynomial of degree d. Further assume that f splits over S, i.e. there are $x_1, \ldots, x_d \in S$ such that f takes the form

$$(t - x_1) \ldots (t - x_d) \;=\; f(t) \;=:\; t^d + a_1 t^{d-1} + \cdots + a_d$$

If now $s \in R[t_1, \ldots, t_d]$ is a symmetric polynomial, then there is a polynomial $h \in R[t_1, \ldots, t_d]$ such that s evaluated on the roots $x_1, \ldots, x_d$ is the same as h evaluated on the coefficients $a_1, \ldots, a_d$

$$s(x_1, \ldots, x_d) \;=\; h(a_1, \ldots, a_d) \;\in\; R$$

(7.68) Proposition: (viz. 808)
Consider a $(R, +, \cdot)$ commutative ring, that contains the rationals $\mathbb{Q} \subseteq R$ [in other words the integers of R are invertible: $\zeta : \mathbb{Z} \hookrightarrow R^*$]. If now $f \in R[t_1, \ldots, t_n]$ is a polnomial over R, where $1 \leq n \in \mathbb{N}$, then we define its **symmetrization** reps. its **anti-symmetrization** to be the following polynomial again

$$\begin{aligned} f_{\mathrm{sym}} \;&:=\; \frac{1}{n!} \sum_{\sigma \in S_n} \sigma f \\ f_{\mathrm{asym}} \;&:=\; \frac{1}{n!} \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma)\, \sigma f \end{aligned}$$

Thereby $f_{\mathrm{sym}} \in R[t_1, \ldots, t_n]_{\mathrm{sym}}$ and $f_{\mathrm{asym}} \in R[t_1, \ldots, t_n]_{\mathrm{asym}}$ truly are symmetric resp. anti-symmetric polynomials and the symmetrization of f equals f if and only if f was symmetric beforehand (likewise for anti-symmetric polynomials)

$$\begin{aligned} f \;=\; f_{\mathrm{sym}} \quad &\Longleftrightarrow \quad f \;\in\; R[t_1, \ldots, t_n]_{\mathrm{sym}} \\ f \;=\; f_{\mathrm{asym}} \quad &\Longleftrightarrow \quad f \;\in\; R[t_1, \ldots, t_n]_{\mathrm{asym}} \end{aligned}$$

Nota as $S : f \mapsto f_{\mathrm{sym}}$ is R-linear we thereby find, that S is a projection $S^2 = S$ on the R-module $R[t_1, \ldots, t_n]$ with image $R[t_1, \ldots, t_n]_{\mathrm{sym}}$. Likewise the same is true for $A : f \mapsto f_{\mathrm{asym}}$.

7.6 Derivations

(7.69) Definition:
Let $(R,+,\cdot)$ be a commutative ring and A be an R-algebra, then a map d of the form $d : A \to A$ is said to be a **derivation** on A, iff it satisfies the following two properties

(1) d is R-linear

(2) For any $f, g \in A$ we get $d(f \cdot g) = d(f) \cdot g + f \cdot d(g)$

Property (2) is called the *product rule* of a derivation. The set of all derivations on A (which is a sub-module of $\mathrm{end}(A)$ the R-module endomorphisms of A) is denoted, by

$$\mathrm{der}(A) \;:=\; \{\, d : A \to A \mid (1) \text{ and } (2) \,\}$$

Nota however $\mathrm{der}(A)$ is *not* a sub-algebra of $\mathrm{end}(A)$, as the composition $d_2 d_1$ does not satisfy the product rule any more, but we rather get

$$(d_2 d_1)(f \cdot g) \;=\; d_2\big(d_1(f \cdot g)\big) \;=\; d_2 d_1 f \cdot g + d_1 f \cdot d_2 g + d_2 f \cdot d_1 g + f \cdot d_2 d_1 g$$

(7.70) Proposition: (viz. 826)
Let R be a commutative ring and A be an R-algebra. Denote the neutral elements of addition and multiplication on A be 0_A and 1_A respectively. If now $d \in \mathrm{der}(A)$ is any derivation on A, then we get the following properties

(i) For any $a \in R$ we have $d(a1_A) = 0_A$

(ii) *General product rule*: For any $f_1, \ldots, f_n \in A$ we have

$$d\big(f_1 \cdot \ldots \cdot f_n\big) \;=\; \sum_{i=1}^{n} f_1 \cdot \ldots \cdot f_{i-1} \cdot d(f_i) \cdot f_{i+1} \cdot \ldots \cdot f_n$$

(iii) If A is a commutative R-algebra containing $f, g \in A$ and $m, n \in \mathbb{N}$ are numbers, such that $n \geq 1$, then any derivation $d \in \mathrm{der}(A)$ satisfies the following two identities

$$\begin{aligned} d\big(f^n\big) &= n d(f) \cdot f^{n-1} \\ d^m\big(f \cdot g\big) &= \sum_{k=0}^{m} \binom{m}{k} d^k(f) \cdot d^{m-k}(g) \end{aligned}$$

(iv) *Quotient rule:* If A is a commutative R-algebra and $U \subseteq A$ is a multiplicatively closed set, that does not contain any zero-divisors $U \cap \mathrm{zd}(A) = \emptyset$, then any derivation $d \in \mathrm{der}(A)$ can be extended to a derivation $U^{-1}d \in \mathrm{der}(U^{-1}A)$ by letting

$$U^{-1}d\left(\frac{f}{u}\right) \;:=\; \frac{d(f) \cdot u - f \cdot d(u)}{u^2}$$

And thereby we get $(U^{-1}d)(f/1) = d(f)/1$ for any $f \in A$. That is we can reconstruct d from $U^{-1}d$ and therefore - by abuse of notation - it is customary to denote $U^{-1}d$ by d again.

(v) If A is a commutative R-algebra and $U \subseteq A$ is a multiplicatively closed set, that does not contain any zero-divisors $U \cap \mathrm{zd}(A) = \emptyset$, then this extension is injective R-module homomorphism from the derivations of A into the derivations of $U^{-1}A$

$$\mathrm{der}(A) \hookrightarrow \mathrm{der}(U^{-1}A) \; : \; d \mapsto U^{-1}d$$

And thereby the image of this monomorphism is given to be the set of all derivations D of $U^{-1}A$, such that for any $f \in A$ there is some $f' \in A$ such that $D(f/1) = f'/1$, formally

$$\Big\{ U^{-1}d \mid d \in \mathrm{der}(A) \Big\} \;\; = \;\; \Big\{ D \in \mathrm{der}(U^{-1}A) \mid \forall\, f \in A \; \exists\, f' \in A \; : \; D(f/1) = f'/1 \Big\}$$

(7.71) Example: (viz. 829)
The classical example is the following: Let $(R, +, \cdot)$ be a commutative ring and regard $A := R[t]$ the polynomial ring over R. Then we obtain a derivation d on A by defining $d(f) := f'$, where

$$f' \;\; := \;\; \sum_{k=1}^{\infty} k f[k]\, t^{k-1} \;\; \in \;\; R[t]$$

(7.72) Definition:
Let $(R, +, \cdot)$ be a commutative ring, fix $1 \leq n \in \mathbb{N}$ and $i \in 1 \ldots n$ and regard the polynomial ring $R[t_1, \ldots, t_n]$. Then we define a derivation ∂_i called the **formal derivative** with respect to the variable t_i in the following way: For any polynomial $f \in R[t_1, \ldots, t_n]$ write f as a polynomial in t_i over a polynomial ring in $n-1$ variables, that is $f \in R[t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_n][t_i]$, then we define $\partial_i f := f'$, that is

$$\partial_i f \;\; = \;\; \sum_{k=1}^{\infty} \left(\sum_{\alpha_i = k} f[\alpha] \prod_{j \neq i} t_j^{\alpha_j} \right) k\, t_i^{k-1}$$

where the sum runs over all $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ with $\alpha_i = k$ and the product runs over the finite set $j \in \{ 1, \ldots, n \} \setminus \{ i \}$. In other words, we define ∂_i by linear expansion of the following assignment of the basis $\{ t^\alpha \mid \alpha \in \mathbb{N}^n \}$ of monomials of $R[t_1, \ldots, t_n]$: Abbreviate $\delta_i = (\delta_{i,j}) \in \mathbb{N}^n$ then $\partial_i t^\alpha$ is

$$\partial_i t^\alpha \;\; := \;\; \begin{cases} 0 \text{ if } \alpha_i = 0 \\ \alpha_i\, t^{\alpha - \delta_i} \text{ if } \alpha_i \geq 1 \end{cases}$$

By (7.73.(i)) all the formal derivatives ∂_i and ∂_j are mutually commutative and hence it makes sense to define their products ∂^α for any multi-index $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ by

$$\partial^\alpha \;\; := \;\; \prod_{i=1}^{n} \partial_i^{\alpha_i} \;\; \in \;\; \mathrm{end}(R[t_1, \ldots, t_n])$$

Nota if we need to emphasize the variable t_i the formal derivative ∂_i acts on, we sometimes use the following, more elaborate, notation for the formal derivative instead

$$\frac{\partial f}{\partial t_i} \;\; = \;\; \frac{\partial}{\partial t_i} f \;\; := \;\; \partial_i f$$

(7.73) Proposition: (viz. 830)
Let $(R,+,\cdot)$ be a commutative ring and $1 \leq n \in \mathbb{N}$. Recall that for $\alpha = (\alpha_1,\ldots,\alpha_n) \in \mathbb{N}$ we defined $\alpha! = \prod_i \alpha_i!$. Then the partial derivatives ∂_i for $i \in 1\ldots n$ satisfy all of the following properties

(i) For any $i, j \in 1\ldots n$ the partial derivatives ∂_i and ∂_j commute, that is for all $f \in R[t_1,\ldots,t_n]$ we have the identity $\partial_i(\partial_j(f)) = \partial_j(\partial_i(f))$.

(ii) Consider any two multi-indices $\alpha = (\alpha_1,\ldots,\alpha_n)$ and $\beta = (\beta_1,\ldots,\beta_n) \in \mathbb{N}^n$. If there is some $i \in 1\ldots n$ such that $\alpha_i > \beta_i$ then we get $\partial^\alpha t^\beta = 0$. And if $\alpha_i \leq \beta_i$ for any $i \in 1\ldots n$ then we obtain the following identity

$$\partial^\alpha t^\beta \;=\; \frac{\beta!}{(\beta-\alpha)!}\, t^{\beta-\alpha}$$

(iii) If R is an integral domain then $\{\,\partial_1,\ldots,\partial_n\,\}$ is algebraically independent, that is we find an isomorphism of the commutative algebra $R[\partial_1,\ldots,\partial_n] \subseteq \mathrm{end}(R[t_1,\ldots,t_n])$ to a polynomial ring in n variables of the following form

$$R[d_1,\ldots,d_n] \;\xrightarrow{\sim}\; R[\partial_1,\ldots,\partial_n] \;:\; f \mapsto f(\partial_1,\ldots,\partial_n)$$

(iv) *Chain rule of differentiation:* Consider any $1 \leq m, n \in \mathbb{N}$ and polynomials $g \in R[t_1,\ldots,t_m]$ and (for any $j \in 1\ldots n$) $f_j \in R[s_1,\ldots,s_m]$. Then we get the identity

$$\frac{\partial}{\partial s_i} g(f_1,\ldots,f_n) \;=\; \sum_{j=1}^{n} \frac{\partial f_j}{\partial s_i} \cdot \frac{\partial g}{\partial t_j}(f_1,\ldots,f_n)$$

(v) *Taylor expansion theorem:* If R contains $\mathbb{Q}$ as a sub-ring [that is $\{\,k1_R \mid 1 \leq k \in \mathbb{N}\,\} \subseteq R^*$] and we fix any point $x = (x_1,\ldots,x_n) \in R^n$ then any polynomial $f \in R[t_1,\ldots,t_n]$ can be written in the following form

$$f \;=\; \sum_{\alpha\in\mathbb{N}^n} \frac{1}{\alpha!}\big(\partial^\alpha f\big)(x) \cdot (t-x)^\alpha$$

(7.74) Proposition: (viz. 554)
Let $(R,+,\cdot)$ be a commutative ring and $1 \leq n \in \mathbb{N}$. Then the derivations on the polynomial ring $R[t_1,\ldots,t_n]$ satisfy the following properties

(i) If d_1 and $d_2 \in \mathrm{der}(R[t_1,\ldots,t_n])$ are any derivations on the polynomial ring then (a) $d_1 = d_2$ and (b) for all $i \in 1\ldots n$ we have $d_1(t_i) = d_2(t_i)$ are equivalent.

Proof of (7.74):

(i) The direction (a) $\implies$ (b) is trivial and for (b) $\implies$ (a) it suffices to check $d_1(t^\alpha) = d_2(t^\alpha)$ for any $\alpha \in \mathbb{N}$, due to the R-linearity of both d_1 and d_2. Let us first prove $d_1(t_i^k) = d_2(t_i^k)$ for any $i \in 1\ldots n$ and $k \in \mathbb{N}$, by induction on k:

For $k = 0$ we have $t_i^k = \mathbf{1}$ and thereby by (7.70.(i)) $d_1(\mathbf{1}) = 0 = d_2(\mathbf{1})$. For $k = 1$ the identity $d_1(t_i^k) = d_2(t_i^k)$ is precisely the content of (b). Thus we perform the induction step $k \mapsto k+1$: By the product rule we have

$$d_1\big(t_i^{k+1}\big) \;=\; d_1\big(t_i^k \cdot t_i\big) \;=\; d_1\big(t_i^k\big)\cdot t_i + t_i^k \cdot d_1\big(t_i\big)$$

By the induction hypothesis we have $d_1(t_i^k) = d_2(t_i^k)$ and $d_1(t_i) = d_2(t_i)$ is granted by (b). So if we apply the product rule to d_2 we end up with the same term, as we can replace d_2 by d_1 on the right-hand side and hence the induction is complete.

In particular we have proved the claim in case $n = 1$. For higher n we use induction on n again: Suppose we already have $d_1(t^\alpha) = d_2(t^\alpha)$ for any $\alpha \in \mathbb{N}^{n-1}$, then we continue

$$\begin{aligned} d_1\big(t^\alpha t_n^{\alpha_n}\big) &= d_1\big(t^\alpha\big) \cdot t_n^{\alpha_n} + t^\alpha \cdot d_1\big(t_n^{\alpha_n}\big) \\ &= d_2\big(t^\alpha\big) \cdot t_n^{\alpha_n} + t^\alpha \cdot d_2\big(t_n^{\alpha_n}\big) \;=\; d_2\big(t^\alpha t_n^{\alpha_n}\big) \end{aligned}$$

□

Chevalley - Fundamental Concepts of Algebra Chapter V: V.6 and V.7

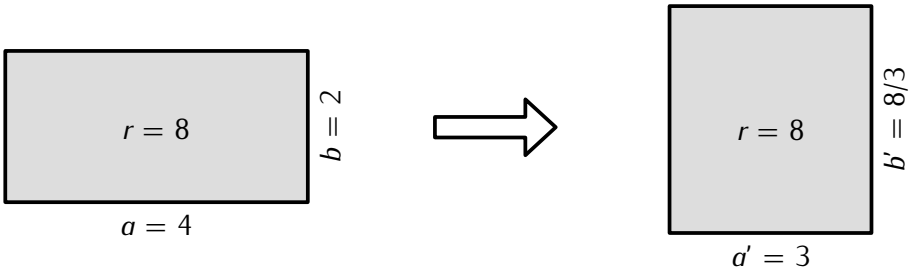
7.7 Gröbner Bases

Monomial Ideals nach Hausen
Buchbergers Algorithmus

7.8 Solution Formulae

Linear algebra set out to provide a theory of solving systems of linear equations, which we finished in section 4.3 to satisfaction. The gaussian algorithm is an efficient way of finding the set of solutions. Alas, this is the one and only situation that allows a definitive answer. Another classical question are polynomial equations in one variable. We will see that even in this case there will not be an ultimate answer, only special cases. So a general theory of solving systems of polynomial equations in several variables is utopic.

The following problem is ancient: Given a positive (real) number $r > 0$, how do you find a root of r, that is a number x such that $x^2 = r$. The following iterative method is described by Heron in the first century AB, already: Interpret r as the area of a rectangle. The length of the sides shall be a and b, that is $ab = r$. What we need is a square of the same area, if x is the side length of the square, we have $x^2 = r$. As one side of the rectangle exceeds x and one falls short it makes sense to take one side as the average $a' = (a+b)/2$. In order to keep the area fixed at r the other side then becomes $b' := r/a'$. The following illustration depicts the situation where $a = 4$ and $b = 2$, that is $r = 8$.



In the next step we get $a' = 3$ and $b' = 8/3$. It can already be seen that the new rectangle is closer to a square, than the one before. So we can iterate and have reason to assume, that we come ever closer to a square. That is by iterating the rectangle over and over we can approximate $x = \sqrt{r}$. So let us take an algebraic look and compute the new value of a' in general

$$a' \;=\; \frac{a+b}{2} \;=\; \frac{a+r/a}{2} \;=\; \frac{a^2+r}{2a}$$

So in modern terms we have found a recursion formula that should converge to $\sqrt{r}$. This might not be wholly satisfactory, but as a and b will stay rational and $\sqrt{r}$ is irrational, this is actually the best, we can hope for. The following proposition tells us, that this method truly yields a way of approximating $x = \sqrt{8}$ to arbitrary precision, as the recursion converges:

(7.75) Proposition: (viz. 836)

(i) Consider any real number $r \in \mathbb{R}$ with $r > 0$. Then there is another, uniquely determined real number $x \in \mathbb{R}$ with $x > 0$ such that $x^2 = r$. And we find a sequence $(a_n) \subseteq \mathbb{Q}$ of rational numbers that converges to $(a_n) \to x$ in the following way: Start with $a_0 := 1$ and use the recursion formula

$$a_{n+1} \;:=\; \frac{a_n^2 + r}{2a_n}$$

(ii) Consider any complex number $z \in \mathbb{C}$ with $z \neq 0$. Then there are exactly 2 complex numbers w_1, $w_2 \in \mathbb{C}$ such that $w_1^2 = z = w_2^2$: Write z in polar coordinates, that is $z = r(\cos(\alpha) + i\sin(\alpha))$, for some $r > 0$ and $\alpha \in \mathbb{R}$. By (i) there is some $x > 0$ with $x^2 = r$, let us denote it by $\sqrt{r} := x$. Then the roots of z are given to be

$$w_{1/2} \;=\; \pm\sqrt{r}\left(\cos\left(\frac{\alpha}{2}\right) + i\sin\left(\frac{\alpha}{2}\right)\right)$$

So in the complex numbers $\mathbb{C}$ the equation $w^2 = z$ always has a (for $z \neq 0$ even 2) solution. In general we cannot expect the equation $x^2 = a$ to have a solution. Even for the reals $\mathbb{R}$, we do not get solutions for $a < 0$. And for the rational numbers $\mathbb{Q}$ even $x^2 = 2$ does not have a solution. But we encountered this before: The equation $2x = 3$ does not have a solution in the integers $\mathbb{Z}$. Our solution was to enhance the integers by fractions, which led to the rationals $\mathbb{Q}$. More generally we introduced the quotient field of an integral domain and even studied localisations. There's nothing wrong with doing this again: The following construction enhances the base ring by picking up a square root ω of an arbitrary element s:

(7.76) Example: (viz. 837)
Let $(R, +, \cdot)$ be a commutative ring and fix any $s \in R$. The following construction yields a ring, called $R[\sqrt{s}]$, such that R can be regarded as a subring of $R[\sqrt{s}]$ and that contains an element $\omega \in R[\sqrt{s}]$ such that $\omega^2 = s$. The construction is simple: We take $R[\sqrt{s}] := R^2$ as an R-module and only need to define the multiplication on $R[\sqrt{s}]$

$$\begin{pmatrix} a \\ b \end{pmatrix}\begin{pmatrix} c \\ d \end{pmatrix} \;:=\; \begin{pmatrix} ac + bds \\ ad + bc \end{pmatrix}$$

Under these operations $R[\sqrt{s}]$ turns into a commutative R-algebra with unit element $1 = (1,0)$. If we take $\omega := (0,1)$, then it is clear, that $\omega^2 = (s,0)$ which we will interpret as s. Note that 1 and ω are the euclidean base elements of R^2 and therefore any element of $R[\sqrt{s}]$ can be written in the form $(a,b) = a + b\omega$ uniquely. In this form the multiplication of $R[\sqrt{s}]$ reads as

$$\big(a + b\omega\big)\big(c + d\omega\big) \;=\; \big(ac + bds\big) + \big(ad + bc\big)\omega$$

Also note that we obtain a monomorphism of rings $R \hookrightarrow R[\sqrt{s}] : a \mapsto (a,0)$ and we use this monomorphism to interpret R as the subring $\{\,(a,0) \mid a \in R\,\}$ of $R[\sqrt{s}]$. In other words $R[\sqrt{s}] : R$ is a ring extension. For $s = -1$ this is precisely the construction used for the complex numbers $\mathbb{C} = \mathbb{R}[\sqrt{-1}]$. We will present two equivalent constructions of the ring $R[\sqrt{s}]$ below. But first for any $a + b\omega \in R[\sqrt{s}]$ let us define $\nu(a + b\omega) := a^2 - sb^2 \in R$. Then the units of $R[\sqrt{s}]$ are given to be those $a + b\omega$ for which $\nu(a + b\omega)$ is a unit in R. And we can use this to compute the inverse of $a + b\omega$, as well: $(a + b\omega)^{-1} = (a^2 - sb^2)^{-1}(a - b\omega)$

$$R[\sqrt{s}]^* \;=\; \{\, a + b\omega \mid a^2 - sb^2 \in R^* \,\}$$

(i) In a first construction we find an isomorphic version of this ring: Start with $R[t]$ the polynomial ring in one variable and take the ideal $\mathfrak{w} := (t^2 - s)R[t]$ in this ring. Then we obtain an isomorphism of R-algebras that maps $1 = (1,0) \mapsto 1 + \mathfrak{w} = 1$ and $\omega = (0,1) \mapsto t + \mathfrak{w}$, given by

$$R[\sqrt{s}] \xrightarrow{\sim} R[t] \Big/ (t^2 - s)R[t] \; : \; a + b\omega \mapsto a + bt + \mathfrak{w}$$

(ii) Another way to look at $R[\sqrt{s}]$ is the following monomorphism of R-algebras, that allows us to interpret $R[\sqrt{s}]$ as a sub-algebra of the matrix ring $\mathrm{mat}_2(R)$

$$R[\sqrt{s}] \hookrightarrow \mathrm{mat}_2(R) \; : \; a + b\omega \mapsto \begin{pmatrix} a & b \\ sb & a \end{pmatrix}$$

(7.77) Proposition: (viz. 839)
Let $(R, +, \cdot)$ be a commutative ring, for any $b \in R$ and $a \in R^*$ let us abbreviate $b/a := ba^{-1} = a^{-1}b$. Also let $R^\square := \{ r^2 \mid r \in R \}$. Now assume that a and $2 := 1 + 1 \in R^*$ are invertible and b, $c \in R$ are arbitrary. Then we regard the following polynomial of degree 2

$$f(t) \;\; := \;\; at^2 + bt + c$$

Let us abbreviate $\Delta := b^2 - 4ac$, then we can rewrite f in its so-called *vertex form*, which is given to be

$$f(t) \;\; = \;\; a\left(t + \frac{b}{2a}\right)^2 - \frac{\Delta}{4a}$$

And thereby we get the following statements: (i) f has no roots in R, if and only if $\Delta \notin R^\square$. (ii) If $\Delta = \omega^2$ for some $\omega \in R$, then f splits over R, as it can be written in the following form

$$f(t) \;\; = \;\; a\left(t + \frac{b+\omega}{2a}\right)\left(t + \frac{b-\omega}{2a}\right)$$

In particular if R is an integral domain and $\omega^2 = \Delta$ again, then the roots of f are uniquely determined:

$$\mathbb{V}(f) \;\; = \;\; \left\{ \frac{-b-\omega}{2a}, \frac{-b+\omega}{2a} \right\}$$

(7.78) Remark:

(i) The above proposition (7.77) provides the theory of solving polynomial equations in one variable of degree 2. For example take the complex numbers $\mathbb{C}$ as the base ring and regard the equation

$$az^2 + bz + c \;\; = \;\; 0$$

where a, b and $c \in \mathbb{C}$ and $a \neq 0$. We want to find the solutions $z \in \mathbb{C}$ of this equation. To do this compute $\Delta := b^2 - 4ac$. If $\Delta = 0$, then clearly $\omega := 0$ satisfies $\omega^2 = \Delta$. And if $\Delta \neq 0$ then write Δ in polar coordinates $\Delta = r(\cos(\alpha) + i\sin(\alpha))$, where $r > 0$ and $\alpha \in \mathbb{R}$. Then by (7.75.(ii)) admits

a root $\omega = \sqrt{\Delta}$, that is we get $\omega^2 = \Delta$ by taking

$$\omega \;:=\; \sqrt{r}\left(\cos\left(\frac{\alpha}{2}\right) + i\sin\left(\frac{\alpha}{2}\right)\right)$$

Now that we have the square root ω of the determinant Δ we know by (7.77) again, that the solution(s) z of the above quadratic equation are given to be

$$z_{1/2} \;=\; \frac{-b \pm \omega}{2a}$$

(ii) In case of the real numbers $\mathbb{R}$ things are a little more restrained: Again let a, b and $c \in \mathbb{R}$ with $a \neq 0$. As above in (i) we look for solutions $x \in \mathbb{R}$ of the equation

$$ax^2 + bx + c \;=\; 0$$

Again let $\Delta := b^2 - 4ac$. If $\Delta = 0$ then take $\omega := 0$ again. And if $\Delta > 0$, then (7.75.(i)) tells us that Δ has a uniquely determined square root $\omega := \sqrt{\Delta} > 0$. That is to say $\omega^2 = \Delta$. And thereby we find the solution(s) of the above quadratic equation to be literally the same

$$x_{1/2} \;=\; \frac{-b \pm \omega}{2a}$$

However, in case $\Delta < 0$, there is no $\omega \in \mathbb{R}$ with $\omega^2 = \Delta$ and thereby this equation does not have any solutions in $\mathbb{R}$. What we can do, is take to $\Delta \in \mathbb{C}$: Here Δ has a root, namely $\omega := i\sqrt{-\Delta}$. And with this ω is stow, the formula for $x_{1/2}$ yields the solutions of the quadratic equation in $\mathbb{C}$.

bla bla Einheitswurzeln

Wurzeln:

$$\{\, x \in \mathbb{R} \mid x^n = 1 \,\} = \begin{cases} \{\, 1 \,\} \text{ if } 2 \mid n \\ \{\, -1, +1 \,\} \text{ if } 2 \not| \, n \end{cases}$$

$$\{\, x \in \mathbb{R} \mid x^n = r \,\} = \begin{cases} \emptyset \text{ if } 2 \mid n, r < 0 \\ \{\, \sqrt[n]{r} \,\} \text{ if } 2 \mid n, r \geq 0 \\ \{\, -\sqrt[n]{r}, +\sqrt[n]{r} \,\} \text{ if } 2 \not| \, n \end{cases}$$

$$\{\, z \in \mathbb{C} \mid z^n = 1 \,\} = \left\{ \exp\left(\frac{2\pi k i}{n}\right) \;\middle|\; k \in 0 \ldots n-1 \right\}$$

$$\left\{ z \in \mathbb{C} \mid z^n = r \cdot e^{i\varphi} \right\} = \left\{ \sqrt[n]{r} \exp\left(\frac{(\varphi + 2\pi k)i}{n}\right) \;\middle|\; k \in 0 \ldots n-1 \right\}$$

$$(x^n - \omega^n) \;=\; (x - \omega) \cdot \left(\sum_{k=0}^{n-1} \omega^{n+1-k} x^k \right)$$

Lösungsformeln für Grad 1 bis 4

what to do with higher degree polynomials

7.9 Irreducibility Tests

(7.79) Proposition: (viz. 840)

(i) If $f \in \mathbb{C}[t]$ is a polynomial with coefficients in the complex numbers and $\overline{f} \in \mathbb{C}[t]$ is the polynomial with $\overline{f}[k] = \overline{f[k]}$ for any $k \in \mathbb{N}$, then $f + \overline{f} \in \mathbb{R}[t]$ and $f\overline{f} \in \mathbb{R}[t]$. And if $z \in \mathbb{C}$ is any complex number, then we get

$$\overline{f}(z) \;=\; \overline{f(\overline{z})}$$

(ii) If $p \in \mathbb{R}[t]$ is a polynomial of odd degree $\deg(p) = 2m + 1$ (for some $m \in \mathbb{N}$) with coefficients in the reals $\mathbb{R}$, then there is some $x \in \mathbb{R}$ such that $p(x) = 0$.

(iii) If $f \in \mathbb{C}[t]$ is any polynomial of degree $\deg(f) \geq 1$ with coefficients in the complex numbers $\mathbb{C}$, then there is some $z \in \mathbb{C}$ such that $f(z) = 0$.

fragments - algebra - rings: proposition 47 to remark 50, lemma 53 to corollary 55
Fundamentalsatz der Algebra
Ableitung von Polynomen + Eigenschaften repeated roots algebraic multiplicity Resultante Diskriminante

Chapter 8

Ring Extensions

8.1 Basic Notions

The most famous ring extension is $\mathbb{C}$ over $\mathbb{R}$ and this already gets the idea across: There is some base ring $R = \mathbb{R}$ and a larger ring $S = \mathbb{C}$, that contains R. In this case we write $S : R$ spoken S *over* R. Another popular example is the polynomial ring $R[t]$ over some commutative ring R. But let us take a closer look: What does it mean, that R is *contained* in S? Clearly $R \subseteq S$ could be a subset, but this need not be the case. With $R[t] : R$ for example there only is an embedding

$$R \hookrightarrow R[t] \;:\; a \mapsto a\,t^0$$

Another important example is a localization $U^{-1}R : R$ of some commutative ring R. In this case we have a canonical homomorphism again

$$\kappa \;:\; R \to U^{-1}R \;:\; a \mapsto \frac{a}{1}$$

but κ only is injective iff $U \subseteq \text{NZD}(R)$. So in general we may not even expect an embedding of the sub-ring. This is the reason why we give a very general definition of a ring extension $S : R$, even though we usually think of a sub-ring $R \subseteq S$. This will be a fixed homomorphism $\alpha : R \to S$ of rings, but the next lemma tells us this is just the same as an R-algebra S. However you will see, that the intuition of a sub-ring $R \subseteq S$ will work just fine.

(8.1) Lemma: (viz. 1213)

(i) If $(R, +, \cdot)$ is a commutative ring and A a commutative R-algebra, then we obtain the so-called **structural homomorphism** $\alpha : R \to A$ by defining $\alpha(a)$ to be the scalar-multiplication of $a \in R$ and $1_A \in A$ in A. And thereby this α is a homomorphism of ring

$$\alpha \;:\; R \to A \;:\; a \mapsto a\,1_A$$

(ii) If $(R, +, \cdot)$ and $(S, +, \cdot)$ are commutative rings and $\alpha : R \to S$ is a homomorphism of rings, then S can be turned into an R-algebra using the multiplication of $\alpha(a)$ and s in S as scalar multiplication

$$R \times S \to S \;:\; (a, s) \mapsto \alpha(a) \cdot s$$

Nota as $\alpha(a) \in S$ satisfies $\alpha(a) = \alpha(a) \cdot 1_S = a\,1_S$ it is clear, that this α thereby becomes the *structural homomorphism* of S under this scalar multiplication induced by α.

(iii) Let $(R, +, \cdot)$ be a commutative ring and $S \neq 0$ be a non-zero commutative R-algebra. If S is torsion free, as an R-module (that is for any $a \in R$ and any $s \in S$ we have $as = 0$ implies $a = 0$ or $s = 0$) then the structural homomorphism $\alpha : R \to S : a \mapsto a\,1_S$ is injective. If S is an integral domain the converse implication is true, as well.

$$S \text{ is } R\text{-torsion free} \quad \Longrightarrow \quad \alpha \text{ is injective}$$

Nota if we take $R := \mathbb{Z}[r]$ and $S := \mathbb{Z}[r,s]/rs\mathbb{Z}[r,s]$ as an R-algebra induced - in the sense of (ii) - by $\alpha : a(r) \mapsto a(r) + rs\mathbb{Z}[r,s]$, then S is not torsion-free, as $r(s + rs\mathbb{Z}[r,s]) = 0 + rs\mathbb{Z}[r,s]$ by construction, but α is injective, still, as $s \mid rs \mid a(r)$ would imply $s \mid a(r)$, which cannot be.

(8.2) Definition: (viz. 1213)
We call the ordered pair (R, T) a **ring extension** - written, as $T : R$ - iff $(R, +, \cdot)$ is a commutative ring and T is a commutative, unital R-algebra. In this case we interpret R as a sub-ring of T, that is by abuse of notation we sometimes denote the following R-subalgebra of T by R again:

$$R\,1_T \;:=\; \{\, a\,1_T \mid a \in R \,\} \quad \leq_{\mathsf{a}} \quad T$$

The **rank** of $T : R$ is defined to be the rank of T as an R-module and will be denoted by $[T : R]$. The extension $T : R$ is said to be **finite** iff $[T : R] < \infty$, that is iff T is finitely generated, as an R-module.

$$[T : R] \;:=\; \mathrm{rank}_R(T)$$

And finally S is said to be an **intermediate ring** of $T : R$ - written, as $T : S : R$, iff $S \leq_{\mathsf{r}} T$ is a sub-ring of T that also satisfies one of the following three equivalent properties

(a) $\{\, a1_T \mid a \in R \,\} \subseteq S$

(b) for any $a \in R$ and $s \in S$ we get $as \in S$

(c) $S \leq_{\mathsf{a}} T$ is an R-sub-algebra

(8.3) Example:

(i) If $(T, +, \cdot)$ is a commutative ring and $R \leq_{\mathsf{r}} T$ is a sub-ring, then $T : R$ clearly is a ring extension. The scalar multiplication ax where $a \in R$ and $x \in T$ is just the usual multiplication $\cdot$ of T. And an intermediate ring S is just another sub-ring $S \leq_{\mathsf{r}} T$ such that $R \subseteq S$.

(ii) Clearly $\mathbb{C} : \mathbb{R}$ and $\mathbb{R} : \mathbb{Q}$ are ring extensions of fields - these are called *field extensions*. Thereby $\mathbb{R}$ is an intermediate ring of $\mathbb{C} : \mathbb{Q}$. Also $\mathbb{Q} : \mathbb{Z}$ is a ring extension, but not a field extension.

(iii) If $(R,+,\cdot)$ is a commutative ring and $R[t]$ the polynomial ring over R, then we already mentioned, that $R[t] : R$ is a ring extension. This is generally true for any commutative monoid A, which gives rise to the ring extension $R[t \mid A] : R$. Recall that the scalar multiplication is point-wise, that is

$$a \sum_{\alpha \in A} f[\alpha]\, t^{\alpha} \;=\; \sum_{\alpha \in A} a f[\alpha]\, t^{\alpha}$$

(iv) If $(R,+,\cdot)$ is a commutative ring and $U \subseteq R$ is a multiplicatively closed subset, then $U^{-1}R$ is an R-algebra [and thereby a ring extension $U^{-1}R : R$] under the scalar multiplication

$$a\frac{b}{u} \;=\; \frac{ab}{u}$$

Nota that is $U^{-1}R : R$ is induced, by $\kappa : R \mapsto U^{-1}R : a \mapsto a/1 = a1_{U^{-1}R}$. Recall that by (2.116) κ is injective, if and only if $U \subseteq \text{NZD}(R)$ - that is if for any $u \in U$ and any $a \in R$ we get $au = 0 \implies a = 0$. This situation will be generalized in the next example:

(v) The most general and most important example is (8.1.(ii)): If $(R,+,\cdot)$ and $(S,+,\cdot)$ are commutative rings and $\alpha : R \to S$ is a fixed homomorphism of rings, then $S : R$ is a ring-extension taking the multiplication of $\alpha(a)$ and s in S as scalar multiplication

$$as \;:=\; \alpha(a) \cdot s$$

(vi) If $S : R$ is a ring extension and $\alpha : R \to S : a \mapsto a\,1_S$ its structural homomorphism, then this induces another R-algebra homomorphism $\overline{\alpha} : R[t] \to S[t]$ by virtue of (7.12.(iv)).

$$\overline{\alpha}\left(\sum_{k=0}^{\infty} f[k]\, t^k\right) \;:=\; \sum_{k=0}^{\infty} \alpha(f[k])\, t^k$$

By abuse of notation we will denote the $\overline{\alpha}$ by α again and in this sense any ring extension $S : R$ already is accompanied by this ring extension $S[t] : R[t]$. It is clear that this example extends to arbitrary polynomial rings $S[t \mid A] : R[t \mid A]$ over a commutative monoid $(A,+)$, if we take to

$$\overline{\alpha}\left(\sum_{\gamma \in A} f[\gamma]\, t^{\gamma}\right) \;:=\; \sum_{\gamma \in A} \alpha(f[\gamma])\, t^{\gamma}$$

(vii) If R is a commutative ring, M any R-module and $\varphi \in \text{end}(M)$ an R-module endomorphism of M. Then we studied $f(\varphi)$, where $f \in R[t]$ is a polynomial, in (5.40). Thereby

$$S \;:=\; R[\varphi] \;=\; \{\, f(\varphi) \mid f \in R[t] \,\} \;\leq_{\text{r}}\; \text{end}(M)$$

is a commutative ring, as any $f(\varphi)$ commutes with any other $g(\varphi)$, where $f, g \in R[t]$. And $R[\varphi]$ clearly is an R-algebra under the scalar multiplication $a\,f(\varphi) = (af)(\varphi)$ such that we have another ring extension $R[\varphi] : R$.

(viii) If $(S,+,\cdot)$ is a commutative ring and $\mathfrak{u}$, $\mathfrak{v} \trianglelefteq_{\mathsf{i}} S$ are ideals of S such that $\mathfrak{u} \subseteq \mathfrak{v}$, then we obtain another ring-extension of the quotient rings of S

$$S\big/_{\mathfrak{v}} : S\big/_{\mathfrak{u}}$$

under the scalar multiplication $(a+\mathfrak{u})(x+\mathfrak{v}) := ax+\mathfrak{v}$. This is well defined, as $a+\mathfrak{u} = b+\mathfrak{u}$ implies $u := b-a \in \mathfrak{u} \subseteq \mathfrak{v}$ such that $ux \in \mathfrak{v}$ and therefore $bx+\mathfrak{v} = (a+u)x+\mathfrak{v} = ax+ux+\mathfrak{v} = ax+\mathfrak{v}$.

(ix) A special case of (vii) is $\mathfrak{u} = 0$, hereby we have $S/\mathfrak{u} = S$ canonically such that for any ideal $\mathfrak{v} \trianglelefteq_{\mathsf{i}} S$ we have the ring extension (under the scalar multiplication $a(x+\mathfrak{v}) = ax+\mathfrak{v}$)

$$S\big/_{\mathfrak{v}} : S$$

(8.4) Definition: (viz. 1214)
Let $S : R$ be any ring extension and $U \subseteq S$ be an arbitrary subset of S. Then we denote the R-sub-algebra of A *generated* by U by the following symbol

$$R[U] \;:=\; \langle U\rangle_{\mathsf{a}} \;=\; \bigcap \{\, Q \leq_{\mathsf{a}} S \mid U \subseteq Q \,\}$$

Let us give a more explicit construction of the intermediate ring $R[U]$: If $u \in S$ is any element of S then we write $R[u]$ instead of $R[\{\, u \,\}]$ and this is just the image of the evaluation homomorphism by u, that is

$$R[u] \;:=\; \{\, f(u) \mid f \in R[t] \,\} \;=\; \left\{ \sum_{k=0}^{n} a_k u^k \;\middle|\; n \in \mathbb{N},\, a_k \in R \right\}$$

Likewise if $u_1, u_2, \ldots, u_n \in S$ are finitely many elements of S, then we write $R[u_1,\ldots,u_n]$ instead of $R[\{\, u_1,\ldots,u_n \,\}]$ and again this is the image of the evaluation homomorphism in the u_k

$$\begin{aligned} R[u_1,\ldots,u_n] &= \{\, f(u_1,\ldots,u_n) \mid f \in R[t_1,\ldots,t_n] \,\} \\ &= \left\{ \sum_{\alpha\in\mathbb{N}^n} a_\alpha u^\alpha \;\middle|\; n \in \mathbb{N},\, a_\alpha \in R \right\} \end{aligned}$$

also confer to example (7.21) for more comments on this. Clearly this is an intermediate ring of $S : R$, as it is the image of a homomorphism of R-algebras. Finally, for a general subset $U \subseteq S$ we find the intermediate ring of $S : R$ generated by U to be the following: If $U = \emptyset$ then $R[U] = R$ and if $U \neq \emptyset$ is non-empty, $R[U]$ is the union of all finitely generated sub-rings $R[u_1,\ldots,u_n]$ where $u_k \in U$, formally

$$R[U] \;=\; \left\{ f(u_1,\ldots,u_n) \;\middle|\; \begin{array}{l} 1 \leq n \in \mathbb{N}, \\ f \in R[t_1,\ldots,t_n], \\ u_1,\ldots,u_n \in U \end{array} \right\} \;=\; \bigcup \left\{ R[u_1,\ldots,u_n] \;\middle|\; \begin{array}{l} 1 \leq n \in \mathbb{N}, \\ u_1,\ldots,u_n \in U \end{array} \right\}$$

(8.5) Proposition: (viz. 1214)
If $S : R$ is a ring-extension, $u_1, u_2, \ldots, u_n \in S$ are (not necessarily distinct) elements of S and $k \in 1 \ldots n$ then we have the following identity of intermediate rings of $S : R$

$$R[u_1, \ldots, u_k][u_{k+1}, \ldots, u_n] \;=\; R[u_1, \ldots, u_n]$$

Note that the case $k = 0$ is trivial, as we have $R[\emptyset] = R$ as mentioned in the definition above. A little more general: If $U, V \subseteq S$ are subsets of S, then $R[U][V]$ is an intermediate ring of $S : R[U]$ and hence of $S : R$, as well. And for these we have the following identity of sets

$$R[U][V] \;=\; R[U \cup V]$$

(8.6) Lemma: (viz. 1215)
Let $T : R$ be any ring-extension and $S \subseteq T$ be any subset. Then we find that the following three statements are equivalent

(a) $T : S : R$ is an intermediate ring

(b) for any subset $U \subseteq S$ we get $R[U] \subseteq S$

(c) for any $u, v \in S$ we get $R[u, v] \subseteq S$

(8.7) Proposition: (viz. 1216)
Let S be an intermediate ring of the ring extension $T : R$. Also consider some non-empty subsets $X \subseteq S$ and $Y \subseteq T$ of S and T respectively. Then we denote the set $XY := \{\, xy \mid x \in X, y \in Y \,\} \subseteq T$ of point-wise products and thereby obtain the following statements:

(i) If X generates S as an R-module $S = \mathrm{Lh}_R(X)$ and Y generated T as an S-module $T = \mathrm{Lh}_S(Y)$ then XY generates T as an R-module, that is

$$T \;=\; \mathrm{Lh}_R(XY)$$

(ii) If X is R-linearly independent and Y is S-linearly independent, then the set XY of point-wise products is R-linearly independent, as well.

(iii) In particular: If X is an R-basis of S and Y is an S-basis of T, then XY is an R-basis of T.

(iv) Hence in any ring extension $T : R$ with an intermediate ring S the degree of $T : R$ cannot exceed the product of the degrees of $T : S$ and $S : R$. Formally we have the inequality

$$[T : R] \;\leq\; [T : S] \cdot [S : R]$$

And if R and S are fields, then the degree of $T : R$ even equals the product of $T : S$ and $S : R$. That is - if R and S are fields - we have the equality

$$[T : R] \;=\; [T : S] \cdot [S : R]$$

(8.8) Remark:
Consider any ring extension $S : R$ and denote its structural homomorphism by $\alpha : R \to S$. That is we think of R as the sub-ring $\alpha(R) = \{\, a\,1_S \mid a \in R \,\}$ of S. Then by (8.3.(vi)) this gives rise to another ring extension $S[t] : R[t]$. In this sense: If $g_1, \ldots, g_r \in S[t]$ are polynomials, then $g_1 \cdot \ldots \cdot g_r \in R[t]$ means

$$\forall\, k \in \mathbb{N} \;\; : \;\; \big(g_1 \cdot \ldots \cdot g_r\big)[k] \;\in\; \alpha(R)$$

And likewise, if $f \in R[t]$ then in $g_1 \cdot \ldots \cdot g_r = f$ the left-hand side polynomial lies in $S[t]$ and the right-hand side polynomial lies in $R[t]$. To say that they are equal means

$$\forall\, k \in \mathbb{N} \;\; : \;\; \big(g_1 \cdot \ldots \cdot g_r\big)[k] \;=\; \alpha(f[k])$$

(8.9) Proposition: (viz. 1225)
If $S : R$ is ring extensions under its structural homomorphisms $\alpha : R \to S$ and $f \in R[t]$ is a polynomial over R, then we say that f **splits** over S, iff there are elements $s_1, \ldots, s_n \in S$ such that f can be written as a product of the linear factors $t - s_k$, formally that is

$$f(t) \;\;=\;\; \mathrm{lc}(f) \prod_{k=1}^{n} \big(t - s_k\big)$$

And if $T : S$ is another ring extensions under the structural homomorphism $\beta : S \to T$, then we regard $T : S$ as a ring extension under $\beta\alpha : R \to T$. Thereby, if $f \in R[t]$ splits over S (as above), then it also splits over T, as we get

$$f(t) \;\;=\;\; \mathrm{lc}(f) \prod_{k=1}^{n} \big(t - \beta(s_k)\big)$$

(8.10) Lemma: (viz. 1217)

(i) *Lemma of Kronecker*: If $(R, +, \cdot)$ is any commutative ring and $f \in R[t]$ is a monic polynomial of degree $n := \deg(f) \geq 1$. Then we take a look at the R-algebra

$$S \;\;:=\;\; R[t] \,\Big/\, fR[t]$$

Thereby $S : R$ is a ring-extension, in which we can consider R as a sub-ring under the monomorphism $\alpha : R \hookrightarrow S : a \mapsto at^0 + fR[t]$ of rings. Also S is a free, finitely generated R-module of dimension $[S : R] = n$. An R-basis of S is given by the following set

$$\Big\{\, t^k + fR[t] \mid 0 \leq k < n \,\Big\}$$

(ii) If $(R, +, \cdot)$ is any commutative ring and $f \in R[t]$ is a monic polynomial of degree $n = \deg(f) \geq 1$ again, then there is another commutative ring $(S, +, \cdot)$ satisfying the following three properties:

(1) $S : R$ can be turned into a ring extension under an injective homomorphism $\alpha : R \hookrightarrow S$

(2) S is finitely generated, as an R-module, its rank being bound by $[S : R] \leq n!$

(3) The polynomial f *splits* over S, that is: There are elements $s_1, \ldots, s_n \in S$ such that f can be written as a product of linear factors of the form $t - s_k$ over S, formally

$$f(t) \;=\; \prod_{k=1}^{n} (t - s_k)$$

(iii) If $(R, +, \cdot)$ is any commutative ring and $f_1, \ldots, f_r \in R[t]$ are monic polynomials of the degrees $n(i) = \deg(f_i) \geq 1$ again, then there is another commutative ring $(S, +, \cdot)$ satisfying

(1) $S : R$ can be turned into a ring extension under an injective homomorphism $\alpha : R \hookrightarrow S$

(2) S is finitely generated, as an R-module, in other words $[S : R] < \infty$

(3) All the polynomials f_1 to f_r *split* over S simultaneously, that is: For any $i \in 1 \ldots r$ there are elements $s_{i,j} \in S$ (where $j \in 1 \ldots n(i)$) such that f_i can be written as a product of linear factors of the form $t - s_{i,j}$ over S, formally again

$$f_i(t) \;=\; \prod_{j=1}^{n(i)} (t - s_{i,j})$$

(iv) If $(E, +, \cdot)$ is a field and $f \in E[t]$ is any polynomial of $n := \deg(f) \geq 1$, then there even is another field $(F, +, \cdot)$ satisfying the following three properties:

(1) $F : E$ can be turned into a ring extension under an injective homomorphism $\alpha : E \hookrightarrow F$

(2) F is finitely generated, as an E-vector-space, its dimension being bound by $[F : E] \leq n!$

(3) The polynomial f *splits* over F, that is: There are elements $a \in E^*$ and $x_1, \ldots, x_n \in F$ such that f can be written as a product of linear factors of the form $t - x_k$ over F, formally

$$f(t) \;=\; a \prod_{k=1}^{n} (t - x_k)$$

(8.11) Remark:

(i) The property that $f \in R[t]$ is a *monic* polynomial is absolutely crucial for this result. If we start with $2t - 1 \in \mathbb{Z}[t]$, then $\mathbb{Z}[t] \twoheadrightarrow \mathbb{Z}[1/2] : g \mapsto g(1/2)$ has the kernel $f\mathbb{Z}[t]$, such that $\mathbb{Z}[t]/f\mathbb{Z}[t]$ and $\mathbb{Z}[1/2]$ are isomorphic. Yet $\mathbb{Z}[1/2]$ is not finitely generated over $\mathbb{Z}$. Also refer to (8.27) for this.

(ii) The benefit of this construction is the following: Let R be any commutative ring and $f \in R[t]$ be a monic polynomial over R. It may happen that f does not have any root in R, such as $f(t) = t^2 + 1 \in \mathbb{R}[t]$. We now extend R to S, thereby R is embedded into S by virtue of

$$R \hookrightarrow S \;:\; a \mapsto at^0 + fR[t]$$

But if we take $x := t + fR[t]$, then $x \in S$ and x is a root of f, as now $f(x) = f(t + fR[t]) = f(t) + fR[t] = 0 + fR[t]$. That is we have found a larger ring S, that contains R, in which f has a root. Starting with $R = \mathbb{R}$ and $f(t) = t^2 + 1 \in \mathbb{R}[t]$ this is the construction that yielded $S = \mathbb{C}$.

(iii) Iterating (i) is precisely the method we used to find the splitting ring S of f in (ii), by inductively building up S, adding one root s_1 at a time and proceeding with the rest f without $(t - s_1)$. This result has a sister-theorem in the case of fields, where $f \in E[t]$ splits in a field extension $F : E$.

(iv) Consider the R-module endomorphism $\varphi : S \to S : s \mapsto xs$ where $x = t + fR[t]$ again. Then the R-basis $\{ 1, x, \ldots, x^{n-1} \}$ of S in (i) is just the cyclic basis $\{ \varphi^k(x) \mid 0 \leq k < n \}$ of x under φ. In this light (i) here and (5.57.(iii)) are much the same result, in different settings.

8.2 Transfer of Ideals

(8.12) Definition:
Let $(R,+,\cdot)$ and $(S,+,\cdot)$ be commutative rings and $\alpha : R \to S$ be a fixed homomorphism of rings, between these. If now $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ is an ideal of R and $\mathfrak{u} \trianglelefteq_{\mathrm{i}} S$ is an ideal of S. Then we define the **pull-back** $\mathfrak{u} \cap R$ of $\mathfrak{u}$ and the **push-forward** $\mathfrak{a}S$ of $\mathfrak{a}$ to be the following ideals of R and S respectively:

$$\mathfrak{u} \cap R \;:=\; \alpha^{-1}(\mathfrak{u}) \;=\; \{\, a \in R \mid \alpha(a) \in \mathfrak{u} \,\}$$

$$\mathfrak{a}S \;:=\; \langle \alpha(\mathfrak{a}) \rangle_{\mathrm{i}} \;=\; \langle \alpha(a) \mid a \in \mathfrak{a} \rangle_{\mathrm{i}}$$

Nota thereby $\mathfrak{u} \cap R \trianglelefteq_{\mathrm{i}} R$ is an ideal, according to proposition (1.76.(vii)) and $\mathfrak{a}S \trianglelefteq_{\mathrm{i}} S$ is an ideal, as it has been defined as the ideal generated by the subset $\alpha(\mathfrak{a}) \subseteq S$. This means that any element $f \in \mathfrak{a}S$ is of the following form for some $s_1,\ldots,s_n \in S$ and $a_1,\ldots,a_n \in \mathfrak{a}$:

$$f \;=\; \alpha(a_1)\cdot s_1 + \cdots + \alpha(a_n)\cdot s_n$$

(8.13) Remark:
If $(S,+,\cdot)$ is any ring and $R \leq_{\mathrm{r}} S$ is a subring, then of course $R \subseteq S$ is a subset. The inclusion map of sets $\iota : R \to S : a \mapsto a$ is a homomorphism of rings, that turns $S : R$ into a ring extension (well, this means S should be commutative). For this structural homomorphism we get $\iota^{-1}(\mathfrak{u}) = \{\, a \in R \mid a \in \mathfrak{u} \,\} = \mathfrak{u} \cap R$ are identical *as sets*, for any subset $\mathfrak{u} \subseteq S$. This is where the notation of the pull-back comes from: In case of ambiguity the pull-back and intersection yield precisely the same ideal.

Likewise if the structural homomorphism $\alpha : R \hookrightarrow S$ is injective, then we get an isomorphic copy $\iota(R) \subseteq S$ of R inside S. Then for any ideal $\mathfrak{u} \trianglelefteq_{\mathrm{i}} S$ we can look at the intersection $\mathfrak{u} \cap \iota(R) \trianglelefteq_{\mathrm{i}} \iota(R)$ of sets. Then $\iota(\iota^{-1}(\mathfrak{u})) = \mathfrak{u} \cap \iota(R)$, that is the pull-back $\iota^{-1}(\mathfrak{u})$ is just the preimage of $\mathfrak{u} \cap \iota(R)$ inside R. Thus the pull-back $\mathfrak{u} \cap R$ is an isomorphic copy of an intersection $\mathfrak{u} \cap \iota(R)$ of sets, inside R. The only real difference occurs, whenever α is *not* injective.

(8.14) Proposition: (viz. 1220)
Consider the commutative rings $(R,+,\cdot)$ and $(S,+,\cdot)$, an arbitrary subset $A \subseteq R$ and a homomorphism $\alpha : R \to S$ of rings. Let $\mathfrak{a} := \langle A \rangle_{\mathrm{i}} \trianglelefteq_{\mathrm{i}} R$ be the ideal generated by A, then the push-forward of $\mathfrak{a}$ is just the ideal of S generated by $\alpha(A)$:

$$\mathfrak{a}S \;=\; \langle \alpha(A) \rangle_{\mathrm{i}} \;\trianglelefteq_{\mathrm{i}}\; S$$

(8.15) Proposition: (viz. 1220)
Let $(R,+,\cdot)$ and $(S,+,\cdot)$ be commutative rings and $\alpha : R \to S$ be a fixed homomorphism of rings, between these. Then the transfer of ideals forms a covariant Galois connection

$$\begin{array}{rcl} \mathrm{Ideal}(R) & \to & \mathrm{Ideal}(S) \\ \mathfrak{a} & \mapsto & \mathfrak{a}S \\ \mathfrak{u} \cap R & \hookleftarrow & \mathfrak{u} \end{array}$$

That is for any ideals $\mathfrak{a}$, $\mathfrak{b} \trianglelefteq_{\mathrm{i}} R$ we find that $\mathfrak{a} \subseteq \mathfrak{b}$ implies $\mathfrak{a}S \subseteq \mathfrak{b}S$. Likewise for any ideals $\mathfrak{u}$, $\mathfrak{v} \trianglelefteq_{\mathrm{i}} S$ we find that $\mathfrak{u} \subseteq \mathfrak{v}$ implies $\mathfrak{u} \cap R \subseteq \mathfrak{v} \cap R$. And finally we have the inclusions

$$\begin{aligned} \mathfrak{a} &\subseteq (\mathfrak{a}S) \cap R \\ (\mathfrak{u} \cap R)\, S &\subseteq \mathfrak{u} \end{aligned}$$

As always in a Galois connection: If $\mathfrak{a} = \mathfrak{u} \cap R$ is the pull-back of some ideal $\mathfrak{u} \trianglelefteq_{\mathrm{i}} S$ then we get $(\mathfrak{a}S) \cap R = \mathfrak{a}$. Likewise if $\mathfrak{u} = \mathfrak{a}S$ is the push-out of some ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$, then we get $(\mathfrak{u} \cap R)S = \mathfrak{u}$. And thereby we obtain a 1-to-1 correspondence, of the form

$$\begin{array}{rcl} \{\, \mathfrak{u} \cap R \mid \mathfrak{u} \trianglelefteq_{\mathrm{i}} S \,\} & \longleftrightarrow & \{\, \mathfrak{a}S \mid \mathfrak{a} \trianglelefteq_{\mathrm{i}} R \,\} \\ \mathfrak{a} & \mapsto & \mathfrak{a}S \\ \mathfrak{u} \cap R & \hookleftarrow & \mathfrak{u} \end{array}$$

For prime ideals this correspondence has even weaker requirements. To be precise, for any prime ideal $\mathfrak{p} \in \operatorname{Spec}(R)$ we find that the above equation holds true if and only if $\mathfrak{p}$ is the pull-back of some prime ideal $\mathfrak{q} \in \operatorname{Spec}(S)$. That is the following two statements are equivalent:

(a) $\mathfrak{p} = (\mathfrak{p}S) \cap R$

(b) $\exists\, \mathfrak{q} \in \operatorname{Spec}(S) \;:\; \mathfrak{p} = \mathfrak{q} \cap R$

(8.16) Remark:

(i) Both of the above inclusions in (8.15) need not be equalities: As a counter-example for the first lets us consider $S := \mathbb{Q}$, $R := \mathbb{Z}$ and $\mathfrak{a} := 2\mathbb{Z}$. Then $1 \in \mathfrak{a}S$ and hence $\mathfrak{a}S = \mathbb{Q}$ such that $\mathfrak{a}S \cap R = \mathbb{Z}$ exceeds $\mathfrak{a}$. As a counter-example for the second let us take to $S := \mathbb{Q}[t]$, $R := \mathbb{Q}$ and $\mathfrak{u} := tS$. Then clearly $\mathfrak{u} \cap R = \{0\}$ such that $(\mathfrak{u} \cap R)S = \{0\}$ is smaller than $\mathfrak{u}$.

(ii) If $S : R$ is any ring extension, then the pull-back $\mathfrak{q} \cap R$ of a prime ideal $\mathfrak{q} \trianglelefteq_{\mathrm{i}} S$ is a prime ideal again, due to (2.17). However the push-out $\mathfrak{p}S$ of a prime ideal $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ need *not* be prime again. As a counter-example, take a look at $\mathbb{Z}[\sqrt{2}] : \mathbb{Z}$ and the prime ideal $2\mathbb{Z} \trianglelefteq_{\mathrm{i}} \mathbb{Z}$. Then the push-out of $2\mathbb{Z}$ is $2\mathbb{Z}[\sqrt{2}]$, but $2 = \sqrt{2} \cdot \sqrt{2}$ no longer is prime.

(8.17) Remark: (viz. 1221)
Let us take a look at a slightly more general situation: Consider homomorphisms of rings, of the form $\iota : R \to S$ and $\pi : S \to R$, such that $\pi\iota = \mathbb{1}_R$. We consider $S : R$ as a ring-extension, induced by ι. If now $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ and $\mathfrak{u} \trianglelefteq_{\mathrm{i}} S$ are ideals, then we obtain the following statements:

(i) π is a homomorphism of R-algebras

(ii) $\mathfrak{a}S \subseteq \pi^{-1}(\mathfrak{a})$

(iii) $\mathfrak{u} \cap R \subseteq \pi(\mathfrak{u})$

However the converse inclusions need not be true: For a counter-example let $R := \mathbb{Q}[x]$ and $S := \mathbb{Q}[x,y]$. Here $\iota : R \to S$ is the canonical inclusion $\iota(f)[\alpha,\beta] = f[\alpha]$ for $\beta = 0$ and $= 0$ for $\beta \neq 0$. And $\pi : S \to R$ is the evaluation homomorphism $\pi(g) = g(x,0)$. Then clearly $\pi\iota(f) = f$.

Now take $\mathfrak{a} := xR$, then $\mathfrak{a}S = xS$ and hence $y \notin \mathfrak{a}S$. However $\pi(y) = 0 \in \mathfrak{a}$ and hence $y \in \pi^{-1}(\mathfrak{a})$. Likewise let $\mathfrak{u} := (y+1)S$, then $\mathfrak{u} \cap R = 0$, as the only $f \in R$ such that $\iota(f)$ is divisible by $y+1$ is $f = 0$. Yet $\pi(y+1) = 1$ and hence $1 \in \pi(\mathfrak{u})$.

(8.18) Proposition: (viz. 1222)
Let $(R,+,\cdot)$, $(S,+,\cdot)$ and $(T,+,\cdot)$ be commutative rings and $\alpha : R \to S$ and $\beta : S \to T$ be homomorphisms of rings. Then we regard $S : R$ and $T : S$ as ring extensions. Likewise $T : R$ is a ring extension induced by $\beta\alpha : R \to T$. If now $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$ and $\mathfrak{c} \trianglelefteq_{\mathfrak{i}} T$ are ideals, then we obtain the following identities concerning the transferred ideals:

$$\begin{aligned} (\mathfrak{a}S)T &= \mathfrak{a}T \\ (\mathfrak{c} \cap S) \cap R &= \mathfrak{c} \cap R \end{aligned}$$

(8.19) Proposition: (viz. 1222)
Consider a homomorphism $\alpha : R \to S$ between the commutative rings R and S. Thus $S : R$ is a ring extension under α and any ideal induces another ring extension on the quotient rings, according to:

(i) If $\mathfrak{u} \trianglelefteq_{\mathfrak{i}} S$ is an ideal and $\mathfrak{a} := \mathfrak{u} \cap R$ is the pull-back of $\mathfrak{u}$, then we obtain a well-defined, injective homomorphism of rings, by virtue of

$$R\big/_{\mathfrak{a}} \hookrightarrow S\big/_{\mathfrak{u}} : a + \mathfrak{a} \mapsto \alpha(a) + \mathfrak{u}$$

(ii) If $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} S$ is an ideal and $\mathfrak{u} := \mathfrak{a}S$ is the push-forward of $\mathfrak{a}$, then we obtain a well-defined, homomorphism of rings and in case $\mathfrak{a} = (\mathfrak{a}S) \cap R$ this homomorphism even is injective

$$R\big/_{\mathfrak{a}} \hookrightarrow S\big/_{\mathfrak{u}} : a + \mathfrak{a} \mapsto \alpha(a) + \mathfrak{u}$$

(8.20) Remark:
If $\alpha : R \twoheadrightarrow S$ is surjective, then clearly the homomorphisms in (i) and (ii) in the proposition above, are surjective, as well - and hence isomorphisms. It may also happen, that they are surjective, even if α is not, e.g. in the case $R = \mathbb{Z}$, $\mathfrak{a} = 2\mathbb{Z}$ and $S = \mathbb{Q}$ we have $\mathfrak{a}\mathbb{Q} = \mathbb{Q}$. But generally this is not the case: Consider any ring A, even the algebraically closed field $A = \mathbb{C}$ and let $R := A[s]$, $\mathfrak{a} := sA[s]$ and $S = A[s,t]$. Then $\mathfrak{a}S = sS$ and thereby we get

$$\begin{array}{ccccc} A & \xrightarrow{\sim} & A[s]\big/_{sA[s]} & \hookrightarrow & A[s,t]\big/_{sA[s,t]} \\ a & \mapsto & a + sA[s] & \mapsto & a + sA[s,t] \end{array}$$

Yet the latter ring is isomorphic, to $A[t] \xrightarrow{\sim} A[s,t]/sA[s,t]$ under $f(t) \mapsto f(t) + sA[s,t]$ and hence the monomorphism is not surjective, it cannot reach any element of the form $tg(s,t) + sA[s,t]$.

(8.21) Proposition: (viz. 1222)
Consider any ring extension $S : R$ and a non-empty index set $\Lambda \neq \emptyset$. For any $\lambda \in \Lambda$ let $\mathfrak{a}_\lambda \trianglelefteq_{\mathrm{i}} R$ be an ideal of R, respectively $\mathfrak{u}_\lambda \trianglelefteq_{\mathrm{i}} S$ be an ideal of S. For ease of notation, also let $\mathfrak{a}$, $\mathfrak{b} \trianglelefteq_{\mathrm{i}} R$ and $\mathfrak{u}$, $\mathfrak{v} \trianglelefteq_{\mathrm{i}} S$ be ideals. Then we find the following statements

(i) The pull-back of ideals is compatible with intersections of ideals. For the sum (of any) and product (of finitely many) ideals, the pull-back still satisfy a one-sided inclusion:

$$\begin{aligned}\left(\bigcap_{\lambda\in\Lambda} \mathfrak{u}_\lambda\right) \cap R &= \bigcap_{\lambda\in\Lambda} (\mathfrak{u}_\lambda \cap R)\\ \left(\sum_{\lambda\in\Lambda} \mathfrak{u}_\lambda\right) \cap R &\supseteq \sum_{\lambda\in\Lambda} (\mathfrak{u}_\lambda \cap R)\\ (\mathfrak{u} \cap R) \cdot (\mathfrak{v} \cap R) &\subseteq (\mathfrak{u} \cdot \mathfrak{v}) \cap R\end{aligned}$$

(ii) The push-out of ideals is compatible with taking sums (of any) and (of finitely many) products of ideals. For the intersection ideals, the push-out still satisfies a one-sided inclusion:

$$\begin{aligned}\left(\bigcap_{\lambda\in\Lambda} \mathfrak{a}_\lambda\right) S &\subseteq \bigcap_{\lambda\in\Lambda} (\mathfrak{a}_\lambda S)\\ \left(\sum_{\lambda\in\Lambda} \mathfrak{a}_\lambda\right) S &= \sum_{\lambda\in\Lambda} (\mathfrak{a}_\lambda S)\\ (\mathfrak{a} S) \cdot (\mathfrak{b} S) &= (\mathfrak{a} \cdot \mathfrak{b}) S\end{aligned}$$

Nota in fact we will prove that the sum of the ideals $\mathfrak{a}_\lambda S$ equals the following set: Let $A \subseteq R$ be the union of the ideals $A := \bigcup_\lambda \mathfrak{a}_\lambda$, then the sum of the ideals contains finite sums of elements of the form $s_i\, \alpha(a_i)$ where $s_i \in S$ and $a_i \in A$. Formally, that is

$$\left(\sum_{\lambda\in\Lambda} \mathfrak{a}_\lambda\right) S = \left\{ \sum_{i=1}^{n} s_i\, \alpha(a_i) \;\middle|\; n \in \mathbb{N},\, s_i \in S,\, a_i \in A \right\}$$

(8.22) Example:
The inclusions in the above proposition may be strict: E.g. consider the ring extension $\mathbb{Z}[t] : \mathbb{Z}$ and regard the ideals $\mathfrak{u}_1 = (t+1)S$ and $\mathfrak{u}_2 = (t-1)S$, where $S = \mathbb{Z}[t]$ of course. Then it is clear, that

$$2 = (t+1) - (t-1) \in (\mathfrak{u}_1 + \mathfrak{u}_2) \cap \mathbb{Z}$$

Yet $\mathfrak{u}_1 \cap \mathbb{Z} = 0$: Suppose there was some $f \in \mathbb{Z}[t]$ such that $g := (t+1)f \in \mathbb{Z}$, then we find $g[0] = f[0]$ and for any $k \geq 1$ also $0 = g[k] = f[k] + f[k-1]$. Thus if $f[0] \neq 0$ is non-zero, then f would not be a polynomial, but a formal power series, as for any $k \geq 1$ we had $f[k] = -f[k-1]$. Likewise $\mathfrak{u}_2 \cap \mathbb{Z} = 0$, as in this case $f[k] = f[k-1]$ for any $k \geq 1$, such that

$$2 \notin 0 = (\mathfrak{u}_1 \cap \mathbb{Z}) + (\mathfrak{u}_2 \cap \mathbb{Z})$$

The counter-example for the intersection is a little more intricate: For the base ring take $R = \mathbb{Z}[t_1, t_2]$ and the ideals $\mathfrak{a}_1 = t_1 R$ and $\mathfrak{a}_2 = t_2 R$. As R is an UFD we have $\mathfrak{a}_1 \cap \mathfrak{a}_2 = t_1 t_2 R$. The extension ring is

$$S \;:=\; R[u] \Big/ (t_1 u - t_2 u) R[u] \;=\; \mathbb{Z}[t_1, t_2, u] \Big/ (t_1 u - t_2 u)\mathbb{Z}[t_1, t_2, u]$$

Let us abbreviate $\mathfrak{v} := (t_1 u - t_2 u)\mathbb{Z}[t_1, t_2, u]$ Then $R \hookrightarrow S$ under $f(t_1, t_2) \mapsto f(t_1, t_2, 0) + \mathfrak{v}$ such that we can even regard R as a subset of S. Let us also abbreviate $s := u + \mathfrak{v} \in S$. Then by (8.14) the ideals $\mathfrak{a}_i S = t_i S$ and $(\mathfrak{a}_1 \cap \mathfrak{a}_2)S = t_1 t_2 S$ are principal again and thereby $t_i s \in \mathfrak{a}_i S$. But by construction we have $t_1 s = t_2 s$ such that we thereby get

$$t_1 s \;\in\; \mathfrak{a}_1 S \cap \mathfrak{a}_2 S$$

However $t_1 s \notin (\mathfrak{a}_1 \cap \mathfrak{a}_2)S = t_1 t_2 S$ - suppose there was some $f \in \mathbb{Z}[t_1, t_2, u]$ such that $t_1 s = t_1 t_2 f + \mathfrak{v} \in S$, then $t_1(t_2 f - u) \in \mathfrak{v}$, but $t_2 f$ can't get rid of the t_2. Hence we have found an element

$$t_1 s \;\notin\; (\mathfrak{a}_1 \cap \mathfrak{a}_2)S$$

Shifting Ideals in Polynomial Rings

We conclude this section by presenting a situation in which the transfer of ideals is particularly well behaved: Ideals in polynomial rings over the same base ring, with differently many variables. Though it is not needed for the rest of this text, this is the algebraic counterpart of regarding an algebraic set in ambient spaces of different dimension.

(8.23) Definition:

If $I \neq \emptyset$ is a non-epmty index set and $(R, +, \cdot)$ is a commutative ring, then we have introduced the polynomial ring $R[t_i \mid i \in I] = R[t \mid \mathbb{N}^{\oplus I}]$ over the monoid $\mathbb{N}^{\oplus I}$ in (7.10). For the time being let us abbreviate this by $R[I]$. And for systematic reasons we would also like to introduce $R[\emptyset] := R$.

If now I and J are any index sets, such that $I \cap J = \emptyset$ [we will usually take $I \subseteq K$ and $J = K \setminus I$ for some set K] then it is clear, that $\mathbb{N}^{\oplus I} \times \mathbb{N}^{\oplus J} = \mathbb{N}^{\oplus (I \cup J)}$ canonically. And by (7.12.(vi)) this gives rise to an isomorphism of R-algebras

$$\begin{array}{ccc} R[u_k \mid k \in I \cup J] & \xrightarrow{\sim} & R[s_i \mid i \in I][t_j \mid j \in J] \\ \displaystyle\sum_{(\alpha,\beta) \in \mathbb{N}^{\oplus I} \times \mathbb{N}^{\oplus J}} f[\alpha, \beta]\, u^{(\alpha,\beta)} & \mapsto & \displaystyle\sum_{\beta \in \mathbb{N}^{\oplus J}} \left(\sum_{\alpha \in \mathbb{N}^{\oplus I}} f[\alpha, \beta]\, s^\alpha \right) t^\beta \end{array}$$

In particular if $I \subseteq K$ are nested index sets, then we let $J := K \setminus I$ and can thereby regard $R[t_i \mid i \in I]$ as a subset of $R[t_k \mid k \in K] = R[t_i \mid i \in I][t_j \mid j \in J]$. This is due to the fact, that the structural homomorphism of the ring extension is injective

$$\iota_I^K \;:\; R[t_i \mid i \in I] \hookrightarrow R[t_k \mid k \in K] \;:\; f \mapsto f\mathbf{1}$$

The coefficients of $f\mathbf{1}$ are given to be $(f\mathbf{1})[\gamma] = f[\alpha]$ whenever $\gamma = (\alpha, 0) \in \mathbb{N}^{\oplus I} \times \mathbb{N}^{\oplus J}$ and $(f\mathbf{1})[\gamma] = 0$, whenever $\gamma = (\alpha, \beta)$ for some $\beta \neq 0$. In the following we are interested in the properties of the transfer of ideals in ring-extensions of the form $R[t_k \mid k \in K] : R[t_i \mid i \in I]$ where $I \subseteq K$. It will turn out, that in this case the transfer of ideals is far better behaved, than in general ring extensions:

(8.24) Proposition: (viz. 1225)
Let $(R, +, \cdot)$ be a commutative ring and I, J and K be arbitrary index sets, such that $I \subseteq J \subseteq K$. By abuse of notation, let us abbreviate $R[I] := R[t_i \mid i \in I]$, likewise $R[J] := R[t_j \mid j \in J]$ and $R[K] := R[t_k \mid k \in K]$. As above let $\iota_I^J : R[I] \hookrightarrow R[J]$ an $\iota_J^K : R[J] \hookrightarrow R[K]$ be the canonical embeddings. Then we get the following statements:

(i) Regardless of the cardinality of I, the polynomial ring always is a union of a net of finitely generated sub-rings of $R[I]$. Formally this can be put as

$$R[I] \;=\; \bigcup \Big\{ \iota_\Omega^I(R[\Omega]) \;\Big|\; \Omega \subseteq I \text{ finite} \Big\}$$

(ii) The canonical embeddings satisfy $\iota_I^K = \iota_J^K \iota_I^J$ and there are homomorphisms $\pi_I^J : R[J] \twoheadrightarrow R[I]$ of R-algebras, that are uniquely determined by the following mapping property for all $j \in J$

$$\pi_I^J(t_j) \;=\; \begin{cases} t_j \text{ if } j \in I \\ 0 \text{ if } j \in J \setminus I \end{cases}$$

And these homomorphism satisfy the properties (1) π_I^J is surjective, (2) $\pi_I^J \iota_I^J = \mathbb{1}_{R[I]}$ and (3) for any ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R[I]$ we get $\pi_I^J(\mathfrak{a}\, R[J]) \subseteq \mathfrak{a}$.

(iii) Consider $f_1, \ldots, f_r \in R[J]$ and $a, a_1, \ldots, a_r \in R[I]$ and let us abbreviate $\widehat{a} := \iota_I^J(a)$ and likewise $\widehat{a}_l := \iota_I^J(a_l) \in R[J]$. If we now have $\widehat{a} = f_1\widehat{a}_1 + \cdots + f_r\widehat{a}_r$ then

$$\exists\, b_1, \ldots, b_r \in R_k \quad \text{such that} \quad a = b_1\, a_1 + \cdots + b_r\, a_r$$

(iv) Expanding an ideal into a larger ring and returning to a smaller ring actually is unaffected by the preceding expansion. Formally, for any ideals $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R[I]$ and $\mathfrak{b} \trianglelefteq_{\mathrm{i}} R[J]$ we get the identities

$$\begin{aligned} \big(\mathfrak{a}\, R[K]\big) \cap R[J] &= \mathfrak{a}\, R[J] \\ \big(\mathfrak{b}\, R[K]\big) \cap R[I] &= \mathfrak{b} \cap R[I] \end{aligned}$$

Nota In the special case $I = J$ we get $(\mathfrak{a}\, R[K]) \cap R[I] = \mathfrak{a}$. That is: If we expand $\mathfrak{a}$ and return, nothing changes. This is far from true for general ring-extensions.

(v) Recall $I \subseteq J$ and let us denote $H := J \setminus I$ and $S := R[I]$. Then we identify $R[J]$ with its isomorphic image $R[J] = R[I][J \setminus I] = S[H]$. If $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R[I]$ is any ideal, then $\mathfrak{a}\, R[J] = \mathfrak{a}[H]$ and we obtain the following isomorphism of R-algebras

$$\mathfrak{a}[H] \;:=\; \Big\{ g \in S[H] \;\Big|\; \forall\, \alpha \in \mathbb{N}^{\oplus H} : g[\alpha] \in \mathfrak{a} \Big\}$$

$$R[J]\,\big/_{\mathfrak{a}\,R[J]} \xrightarrow{\sim} \left(R[I]\,\big/_{\mathfrak{a}}\right)[H] \;:\; g + \mathfrak{a}\,R[J] \mapsto \sum_{\alpha\in\mathbb{N}^{\oplus H}} \big(g[\alpha] + \mathfrak{a}\big)t^{\alpha}$$

Thereby: An ideal $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R[I]$ is prime, if and only if the push-out $\mathfrak{p}\,R[J] \trianglelefteq_{\mathrm{i}} R[J]$ is a prime ideal again. Nota In the special case $I = \emptyset$ we have $S = R$ and $H = J$ and thereby any ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ satisfies $\mathfrak{a}\,R[J] = \mathfrak{a}[J] = \big\{\, g \in R[J] \mid \forall\, \alpha \in \mathbb{N}^{\oplus J} : g[\alpha] \in \mathfrak{a} \,\big\}$.

(vi) Let J be some index set and consider a countable, ascending chain of subsets $I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots$ of indices, that exhaust J. That is J is the union

$$J \;:=\; \bigcup_{n\in\mathbb{N}} I_n$$

Then for an arbitrary ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R[J]$ we find, that $\mathfrak{a}$ is the capstone of the ascending chain of ideals $(\mathfrak{a} \cap R[I_{n-1}])\,R[J] \subseteq (\mathfrak{a} \cap R[I_n])\,R[J]$. This is to say, that

$$\sum_{n=0}^{\infty} \big(\mathfrak{a} \cap R[I_n]\big)\,R[I_\infty] \;=\; \mathfrak{a}$$

8.3 Integral Extensions

The historic origin of the following notions is a classic problem: The *squaring of the circle*: That is we want to find (ideally even to construct) a square, that has the same area, as a given circle. It is well known that the area of a circle of radius r is πr^2 and the area of a square of side length a is a^2. So this amounts to solving the equation

$$a^2 \;=\; \pi r^2$$

to a. The solution is $a = r\sqrt{\pi}$ of course, but this is not so simple, as it may seem to us today: The reals are complete and hence satisfy the supremum property. So $\sqrt{\pi}$ clearly is a *real* number. But classically there only are rational numbers. So the question is: Is $\sqrt{\pi} = a/r$ a *rational* number? In other words still: Does π satisfy a polynomial of the form $t^2 - q \in \mathbb{Q}[t]$ for some $q = a/r \in \mathbb{Q}$?
But maybe this is a little too much to ask for. We could just start with *any* polynomial $f \in \mathbb{Q}[t]$ (apart from $f = 0$ of course) for which $f(\pi) = 0$. So, is there any? It turns out the answer is *no*! For any $f \in \mathbb{Q}[t]$ we have $f(\pi) \neq 0$ unless we started with $f = 0$ in the first place (though the proof of this is far from obvious). This means that π is *not* a combination of algebraic operations (including roots of any power), of rational numbers, whatsoever. In this sense π is outside algebra's reach, if we start from $\mathbb{Q}$. You have to use infinite computations in order to reach it. The following beautiful formula of Leibnitz is an example of this (though its proof is not easy, as well):

$$\frac{\pi}{4} \;=\; 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} + \cdots \;=\; \sum_{k=0}^{\infty} \frac{(-1)^k}{2k+1}$$

Of course we would have to establish a meaning, what an infinite sum is supposed to be, but we leave this to any basic course on analysis. Mathematicians use to say that π is *transcendent* over $\mathbb{Q}$, which is to say that you cannot reach it by finite means. The complementary notion is: If there is some $f \in \mathbb{Q}[t]$ with $f \neq 0$ such that $f(x) = 0$, then x is said to be *algebraic* or *integral* over $\mathbb{Q}$ (we will soon make a slight distinction between these two notions, but over $\mathbb{Q}$ they coincide). All the rational numbers and any roots thereof are examples of this. But there also are exceptions, like π and e.
The notion of being transcendent resp. integral not only is of interest in number fields, where it is the staging point of quite some theory. But it turns out that the same property has deep geometric interpretations and hence is one of the fundamental concepts of algebraic geometry. But we are getting ahead of ourselves, lets start with the basic definitions:

(8.25) Definition: Intergal Extensions:
Let $S : R$ be a ring extension and consider some element $x \in S$. Then x is said to be **algebraic over** R, iff for any element $x \in S$ there is some non-zero polynomial $f \in R[t]$ such that x is a root of this polynomial; formally

$$\exists\; f \in R[t] \;\;:\;\; f \neq 0 \;\text{ and }\; f(x) = 0$$

Now $S : R$ is said to be an **algebraic extension** iff any $x \in S$ is algebraic over R. Somewhat more restrictive: x is said to be **integral over** R iff there is a monic polynomial $m \in R[t]$ such that x is a root of this polynomial. Formally again

$$\exists\; m \in R[t] \;\;:\;\; \mathrm{lc}(m) = 1 \;\text{ and }\; m(x) = 0$$

Likewise $S : R$ is said to be an **integral extension** iff any $x \in S$ is integral over R. The set of all algebraic resp. integral elements of S is said to be the **algebraic closure** (resp. the **integral closure**) of R in S and will be denoted by

$$\begin{aligned} \operatorname{alg}(S:R) &:= \{\, x \in S \mid x \text{ is algebraic over } R \,\} \\ \operatorname{int}(S:R) &:= \{\, x \in S \mid x \text{ is integral over } R \,\} \end{aligned}$$

(8.26) Remark:
Let us take a closer look at the definition above - in other words this reads as: If $x \in S$ is an integral element of the ring extension, then there is a power $1 \leq n \in \mathbb{N}$ and elements $a_0, \ldots, a_{n-1} \in R$ such that

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \;=\; 0$$

In particular: If $a \in R$, then we may take $m(t) := t - a \in R[t]$ to find $m(a) = a - a = 0$. Hence any $a \in R$ of course is integral over R, formally this is the inclusion

$$R\,1_S \;\subseteq\; \operatorname{int}(S:R)$$

If $x \in S$ is algebraic only, then this equation need not be monic, that is there is a power $1 \leq n \in \mathbb{N}$ and elements $a_0, \ldots, a_n \in R$ (as not all the a_k are allowed to be zero we may take $a_n \neq 0$) such that

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \;=\; 0$$

If R is a field then we can divide the respective equation $f(x) = 0$ by the leading coefficient a_n of f. Hence - supposed R is a field - any algebraic extension already is integral. However if R is an integral domain only, then an algebraic extension need not be integral.

(8.27) Example:
Consider the ring extension $\mathbb{Q} : \mathbb{Z}$, then $1/2 \in \mathbb{Q}$ is algebraic over $\mathbb{Z}$, since it is a root of $f(t) = 2t - 1$. However $1/2$ is *not* integral over $\mathbb{Z}$. Suppose we had an equation of the form

$$\left(\frac{1}{2}\right)^n + \sum_{k=0}^{n-1} a_k \left(\frac{1}{2}\right)^k \;=\; 0$$

then multiplying this equation with 2^n and rearranging a little would yield the following equation, which cannot be true, since $2 \notin \mathbb{Z}^*$

$$1 \;=\; -\sum_{k=0}^{n-1} a_k 2^{n-k} \;=\; -2\sum_{k=0}^{n-1} a_k 2^{n-1-k} \;\in\; 2\mathbb{Z}$$

(8.28) Proposition: (viz. 1228)
Let $(Q,+,\cdot)$ and $(S,+,\cdot)$ be commutative rings and $P \leq_r Q$ and $R \leq_r S$ be a sub-rings of Q and S respectively. Also consider an epimorphism of rings $\pi : S \twoheadrightarrow Q$ such that $\varrho(R) \subseteq P$. If now $\star$ abbreviates any one of the words *integral*, *finitely generated* or *finite*, then we get the implication

$$S : R \text{ is } \star \implies Q : P \text{ is } \star$$

Nota In fact we will prove a little more: If $\{ s_i \mid i \in I \} \subseteq S$ generates S as an R-module (resp. R-algebra), then $\{ \pi(s_i) \mid i \in I \}$ generates Q as as a P-module (resp. P-algebra). In particular we find

$$[Q : P] \leq [S : R]$$

(8.29) Proposition: (viz. 1229)
Let $S : R$ be a ring extension and $\mathfrak{u} \trianglelefteq_i S$ be an ideal in the extension ring S. Then we obtain the following statements

(i) If $x \in \text{NZD}(S)$ is a non-zero divisor of S (that is $xy = 0$ implies $y = 0$) and x is integral over R, then there is a monic polynomial $m \in R[t]$ over R, such that $m(x) = 0$ and $m(0) \neq 0$.

(ii) If $S : R$ is an integral extension such that the structural homomorphism $\alpha : R \hookrightarrow S : a \mapsto a\,1_S$ is injective, then $\alpha(R^*) = S^*$. That is for any $a \in R$ we find [and in this case $\alpha(a)^{-1} = \alpha(a^{-1})$]

$$a \in R^* \iff \alpha(a) \in S^*$$

(iii) If $S : R$ is an integral extension and $\mathfrak{u} \cap R = 0$, then $\mathfrak{u}$ is contained in the zero-divisors of S. Formally that is the implication:

$$\mathfrak{u} \cap R = 0 \implies \mathfrak{u} \subseteq \text{ZD}(S)$$

(iv) If $S : R$ is an integral extension then the following ring extension is integral, as well (where the structural homomorphism, given by $\overline{\alpha} : a + \mathfrak{u} \cap R \mapsto \alpha(a) + \mathfrak{u}$, is injective)

$$S \big/ \mathfrak{u} : R \big/ \mathfrak{u} \cap R \text{ is integral}$$

(v) If $U \subseteq R$ is multipicatively closed, then we regard $U^{-1}S$ as an $U^{-1}R$-algebra, as in (3.123). If now $S : R$ is integral, then the ring extension $U^{-1}S : U^{-1}R$ is integral, as well (where the structural homomorphism, is given by $U^{-1}\alpha : a/u \mapsto (a\,1_S)/u = a/u\,1_{U^{-1}S}$)

$$U^{-1}S : U^{-1}R \text{ is integral}$$

(vi) If $(R,+,\cdot)$ is an integral domain and $f \in R[t]$ is a monic polynomial of degree $n := \deg(f) \geq 1$, then $R[t] : R[f]$ is a finite ring extension having the basis $\{ t^k \mid 0 \leq k < n \}$.

(8.30) Lemma: (viz. 1231)
Let $S : R$ be a ring extension. Then we find the following relations between the notions of a *finite*, *integral* or *algebraic* ring extension $S : R$ to be true:

(i) If $x \in S$ is an integral element over R, then $R[x] : R$ is finite. More precisely: If $m \in R[t]$ is a monic polynomial of degree $\deg(m) = n$ such that $m(x) = 0$, then $\{\, x^k \mid 0 \leq k < n \,\}$ is a generating set of $R[x]$ over R and hence $[R[x] : R] \leq n$.

(ii) If $x_1, \ldots, x_n \in S$ are finitely many elements of S, that are integral over R and $P := R[x_1, \ldots, x_n]$ is the intermediate ring generated by these elements, then $[P : R] < \infty$ is a finite extension.

(iii) If $S : R$ is a finite extension, then $S : R$ also is integral. More precisely: If $n = [S : R]$ then for any $x \in S$ there is some monic polynomial $m \in R[t]$ of degree $\deg(m) \leq n$ such that $m(x) = 0$.

(iv) If $S : R$ is a ring extension generated by integral elements, then the entire extension $S : R$ is integral. More precisely: If there is some $X \subseteq S$ such that any $x \in X$ is integral over S and we also have $S = R[X]$, then any $s \in S$ is integral over R.

(v) We find the equivalence: $S : R$ is a finite ring extension (i.e. there are finitely many $s_1, \ldots, s_k \in S$ such that $S = \mathrm{Lh}_R\{\, s_1, \ldots, s_k \,\}$), if and only if $S : R$ is integral and finitely generated (i.e. there are finitely many $x_1, \ldots, x_n \in S$ such that $S = R[x_1, \ldots, x_n]$)

(vi) If $S : R$ is any ring extension, then the set $\overline{R} := \mathrm{int}(S : R) \subseteq S$ of elements of S that are integral over R, is an intermediate ring $S : \overline{R} : R$ of $S : R$. And for this we get

$$\mathrm{int}\big(S : \overline{R}\big) \;=\; \overline{R}$$

(vii) If $S : E$ is any ring extension in which E is a field and $x \in S$ is an algebraic element over E, then $E[x]$ already is a field.

(viii) If $S : R$ is an integral ring extension, where $S \neq 0$ is a non-zero ring, then the following two combinations of properties or R and S are equivalent

(a) R is a field and S is an integral domain

(b) S is a field and S is a torsion-free R-module

Nota As S in (b) also is an integral domain, (8.1.(iii)) tells us that it suffices that the structural homomorphism $\alpha(a) = a\,1_S$ is injective. Then S already is a torsion-free R-module.

Nota If S in (b) is not torsion-free, then R in (a) need not be a field: As a counter-example just look at the ring extension $\mathbb{Z}_7 : \mathbb{Z}_{21}$ in which $\mathbb{Z}_7$ is a field, as $7 \in \mathbb{Z}$ is prime, but $\mathbb{Z}_{21}$ is not.

(ix) Let $S : R$ is any ring extension and denote $\overline{R} := \mathrm{int}(S : R)$ again. If now $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ is an ideal of R and $x \in S$ an element of S, then we say that x is *integral over* $\mathfrak{a}$ iff there are some $n \geq 1$ and $a_0, \ldots, a_{n-1} \in \mathfrak{a}$ such that $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$. And thereby we get

$$\{\, x \in S \mid x \text{ is integral over } \mathfrak{a} \,\} \;=\; \sqrt{\mathfrak{a}\overline{R}}$$

(8.31) Lemma: (viz. 1234)
Let $(R,+,\cdot)$, $(S,+,\cdot)$ and $(T,+,\cdot)$ be commutative rings and $\alpha : R \to S$ and $\beta : S \to T$ be homomorphisms of rings. Then we regard $S : R$ and $T : S$ as ring extensions. Likewise $T : R$ is a ring extension induced by $\beta\alpha : R \to T$. Then the following statements are true:

(i) The property *finitely generated* is transitive, this is to say: If $S : R$ is finitely generated, say $S = R[s_1, \ldots, s_m]$ where $s_i \in S$ and $T : S$ is finitely generated, too, say $T = S[t_1, \ldots, t_n]$ where $t_j \in T$, then $T : R$ is finitely generated, by $T = R[\beta(s_i), \ldots, \beta(s_m), t_1, \ldots, t_n]$, as well.

(ii) If β is injective, then the following two statements (a) and (b) are equivalent: Nota if β is not injective, then we still retain (b) $\implies$ (a) and (a) $\implies$ $T : S$ is integral.

 (a) $T : R$ is integral

 (b) both $T : S$ and $S : R$ are integral

(iii) In the following two statements, we generally have (b) $\implies$ (a). If R is a PID and β is injective, then the statements (a) and (b) are equivalent:

 (a) $T : R$ is finite

 (b) both $T : S$ and $S : R$ are finite

(8.32) Theorem: (viz. 1259)
Lying-over Theorem: Let $S : R$ be any integral ring extension, with $S \neq 0$ and denote its structural homomorphism by $\alpha : R \to S$ with $\alpha(a) = a\,1_S$. Then all the following statements are true:

(i) As always $\Sigma := \operatorname{Spec}(\alpha)$ is well-defined. But since $S : R$ is integral, Σ even is surjective. That is for any prime ideal $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ there is some prime ideal $\mathfrak{q} \trianglelefteq_{\mathrm{i}} S$, such that we get $\mathfrak{p} = \mathfrak{q} \cap R$

$$\Sigma \;:\; \operatorname{Spec}(S) \twoheadrightarrow \operatorname{Spec}(R) \;:\; \mathfrak{q} \mapsto \mathfrak{q} \cap R$$

And if S is a noetherian ring, then Σ only has finite fibres. That is for any prime ideal $\mathfrak{p} \in \operatorname{Spec}(R)$ the fibre $\Sigma^{-1}(\mathfrak{p}) \subseteq \operatorname{Spec}(S)$ is a finite set. Formally this can be put as

$$\forall\, \mathfrak{p} \in \operatorname{Spec}(R) \;:\; \#\{\, \mathfrak{q} \in \operatorname{Spec}(S) \mid \mathfrak{q} \cap R = \mathfrak{p} \,\} < \infty$$

(ii) The restriction $\Sigma : \operatorname{Smax}(S) \twoheadrightarrow \operatorname{Smax}(R)$ is well-defined and surjective, as well. In fact, for any prime ideal $\mathfrak{n} \in \operatorname{Spec}(S)$ we find that: $\mathfrak{n}$ is a maximal ideal of S, if and only if $\mathfrak{n} \cap R \trianglelefteq_{\mathrm{i}} R$ is a maximal ideal of R. Formally

$$\forall\, \mathfrak{n} \in \operatorname{Spec}(S) \;:\; \mathfrak{n} \text{ is maximal} \iff \mathfrak{n} \cap R \text{ is maximal}$$

(iii) The map Σ is somewhat weaker than injective: If $\mathfrak{u}$ and $\mathfrak{v} \trianglelefteq_{\mathrm{i}} S$ are any ideals, such that and one is contained in the other, but $\mathfrak{u} \cap R = \mathfrak{v} \cap R$ is identical and a prime ideal, then $\mathfrak{u}$ and $\mathfrak{v}$ already are equal, themselves:

$$\left.\begin{array}{ccc} \mathfrak{u} & \subseteq & \mathfrak{v} \\ \mathfrak{u} \cap R & = & \mathfrak{v} \cap R \end{array}\right\} \implies \mathfrak{u} = \mathfrak{v}$$

(iv) Let $\mathfrak{b} \trianglelefteq_i S$ be an arbitrary and $\mathfrak{q} \trianglelefteq_i S$ be a prime ideal, then $\mathfrak{b} \subseteq \mathfrak{q}$ is equivalent to $\mathfrak{b} \cap R \subseteq \mathfrak{q} \cap R$. Using $\mathbb{V}(\mathfrak{b}) := \{ \mathfrak{q} \in \mathrm{Spec}(S) \mid \mathfrak{b} \subseteq \mathfrak{q} \}$ this is the following identity of sets of prime ideals of R

$$\Sigma\big(\mathbb{V}(\mathfrak{b})\big) \quad = \quad \mathbb{V}\big(\mathfrak{b} \cap R\big)$$

Nota the $\mathbb{V}(\mathfrak{b})$ can be used as the closed set of a topology on the spectrum $\mathrm{Spec}(S)$, the so-called *Zariski-topology*. In this sense (iv) tells us, that Σ is a *closed* map with respect to the Zariski-topologies on the spectra $\mathrm{Spec}(R)$ and $\mathrm{Spec}(S)$.

(v) For any prime ideals $\mathfrak{p} \trianglelefteq_i R$ and $\mathfrak{q} \trianglelefteq_i S$ we get: If $\mathfrak{p} = \mathfrak{q} \cap R$ then $\mathfrak{p} = (\mathfrak{p}S) \cap R$ and $\mathfrak{q}$ is a minimal prime over $\mathfrak{p}S$. The latter is to say: $\mathfrak{p}S \subseteq \mathfrak{q}$ and for any $\mathfrak{q}' \in \mathrm{Spec}(S)$ we find that $\mathfrak{p}S \subseteq \mathfrak{q}' \subseteq \mathfrak{q}$ implies $\mathfrak{q}' = \mathfrak{q}$. Formally that is

$$\Sigma^{-1}(\mathfrak{p}) \quad \subseteq \quad \mathbb{V}\big(\mathfrak{p}S\big)_*$$

(8.33) Lemma: (viz. 1258)
Lemma of Gauss: Let $S : R$ be any ring extension and abbreviate $\overline{R} := \mathrm{int}(S : R)$. If now $p, q \in S[t]$ are monic polynomials, such that $pq \in \overline{R}[t]$, then $p, q \in \overline{R}[t]$ already.

(8.34) Remark:
Recall that we defined $(R, +, \cdot)$ to be a **normal domain** iff it is an integral domain, that is integrally closed in its quotient field $E := \mathrm{quot}(R)$. That is, the word "domain" refers to property (1), whereas "normal" refers to property (2) of

(1) R is an *integral domain*: $0 \neq 1$ and $\mathrm{zd}(R) = \{0\}$

(2) R is *integrally closed* in E: $\mathrm{int}(E : R) = R$

By now we have seen two situations, that guarantee R to be a normal domain: (i) Any UFD is a normal domain, by (2.65) and (ii) if R is an integral domain, then $\overline{R} := \mathrm{int}(E : R)$ is a normal domain, by (8.30.(vi)). And in this light the Lemma of Gauss (8.33) can be seen, as a generalization of (7.29.(x)). For a normal domain R it can be formulated as:

Lemma of Gauss: Let $(R, +, \cdot)$ be a normal domain and $E := \mathrm{quot}(R)$ its quotient field. If now $p, q \in E[t]$ are monic polynomials, such that $pq \in R[t]$, then $p, q \in R[t]$ already.

Norm and Trace
The following insight is as simple, as it is ingenious: As S in $S : R$ is an R-module and the multiplication on S is R-linear, we can look at the operations of R through the spectacles of linear algebra. This will become one of the cornerstones of Galois Theory that addresses the problem of solving polynomial equations.

(8.35) Remark:
If $S : R$ is a ring extension and $x \in S$, then we obtain an R-linear map on S by multiplication with x (from the left). That is the following map λ_x is an R-module endomorphism of S

$$\lambda_x \ : \ S \to S \ : \ u \mapsto xu$$

The additivity $\lambda_x(u+v) = \lambda_x(u) + \lambda_x(v)$ is due to the first identity in (M) of an R-semi-algebra and the R-linearity $\lambda_x(au) = a\lambda_x(u)$ is part of property (A), there. This map is the link between linear algebra and ring extensions, it will be used to define the characteristic and minimal polynomials of an element $x \in S$: If $f \in R[t]$ is any polynomial and x, $u \in S$, then is is clear that $f(\lambda_x)(u) = f(x)\,u$, as

$$f(\lambda_x)(u) \;=\; \left(\sum_{k=0}^{\infty} f[k]\lambda_x^k\right)(u) \;=\; \sum_{k=0}^{\infty} f[k]\,x^k u \;=\; f(x)\cdot u$$

In other words that is $f(\lambda_x)(u) = f(x)\,u = \lambda_{f(x)}(u)$ and hence $f(\lambda_x) = \lambda_{f(x)}$, as this is true for any $u \in S$. In particular we find that $f(\lambda_x) = 0 \in \mathrm{end}(M)$ is equivalent to $f(x) = 0 \in S$: If $f(\lambda_x) = 0$ then $0 = f(\lambda_x)(1) = f(x)\,1 = f(x)$ and vice versa. Let us emphasize this important equivalence

$$f(\lambda_x) \;=\; 0 \quad\Longleftrightarrow\quad f(x) \;=\; 0$$

Therefore the null ideal $\{\, f \in R[t] \mid f(\lambda_x) = 0 \,\}$ of λ_x is just the same as $\{\, f \in R[t] \mid f(x) = 0 \,\}$ the null ideal of x. In this sense the minimal polynomial of a ring-extension is just a special case of a minimal polynomial of an endomorphism. Nevertheless let us reformulate (5.42.(iii)) for this special case:

(8.36) Definition:
Consider a ring extension $S : R$ where R is an integral domain. For a fixed $x \in S$ we call the kernel $\mathfrak{v}_x$ of the evaluation homomorphism ε_x the **null ideal** of x

$$\varepsilon_x \;:\; R[t] \to S \;:\; f \mapsto f(x)$$

$$\mathfrak{v}_x \;:=\; \{\, f \in R[t] \mid f(x) = 0 \,\} \;\trianglelefteq_{\mathrm{i}}\; R[t]$$

Clearly x is algebraic over R if and only if $\mathfrak{v}_x \neq 0$. And a polynomial $m \in R[t]$ is said to be the **minimal polynomial** of x, iff it satisfies one of the following four equivalent properties. If such a polynomial exists, it is uniquely determined and we write $m_x := m$ again.

(a) The polynomial m satisfies: (1) m is monic, (2) $m(x) = 0$ and (3) for any $f \in R[t]$ we find that $f(x) = 0$ implies $m \mid f$.

(b) The polynomial m satisfies: (1) m is monic, (2) $m(x) = 0$ and (3) for any $f \in R[t]$ with $f \neq 0$ we find that $f(x) = 0$ implies $\deg(m) \leq \deg(f)$.

(c) The polynomial m satisfies: (1) m is monic and (2) m generates the null ideal of x, formally that is: $mR[t] = \{\, f \in R[t] \mid f(x) = 0 \,\}$.

(d) The polynomial m is the minimal polynomial of $\lambda_x \in \mathrm{end}(S)$, $\lambda_x(u) := xu$ in the sense of (5.41.(v)).

Nota As R is an integral domain, $\mathfrak{v}_x \in \mathrm{Spec}(R[t])$ is a prime ideal and if m is the minimal polynomial of x, then we get from (c), that $m \in R[t]$ already is a prime element of the polynomial ring. In short: If it exists, the minimal polynomial always is irreducible.

(8.37) Corollary: (viz. 1258)
Let $S : R$ be a ring extension, in which R is a normal domain. If now $x \in S$ is an element, that is integral over R, then it has has a minimal polynomial $m_x \in R[t]$.

(8.38) Definition:
Let $S : R$ be a finite ring extension, such that S is a free R-module. For any $x \in S$ we regard the homothety $\lambda_x : S \to S : y \mapsto xy$, which is an endomorphism of R-modules. Then we may define the **norm** and **trace** of x to be the determinant resp. trace of this endomorphism λ_x

$$\begin{aligned} N_{S:R}(x) &:= \det(\lambda_x) \\ T_{S:R}(x) &:= \mathrm{tr}(\lambda_x) \end{aligned}$$

Thereby $N_{S:R}$ and $T_{S:R}$ are maps of the form $S \to R$. And in complete analogy we define the **characteristic polynomial** of x to be the characteristic polynomial of λ_x, that is

$$c_x(t) := c_{\lambda_x}(t) = \det(t\mathbb{1}_S - \lambda_x) \in R[t]$$

Nota that both the determinant and trace of $\lambda_x \in \mathrm{end}(S)$ are independent of the specific ordered R-basis chosen for S, according to (4.43). And the same is true for the characteristic polynomial, due to (5.41.(ii)).

(8.39) Proposition: (viz. 975)
Let $S : R$ be a finite ring extension of degree $n := [S : R]$, such that S is a free R-module. Then $T_{S:R} : S \to R$ is R-linear and $N_{S:R} : S \to R$ is multiplicative, that is

$$\begin{aligned} T_{S:R}(ax) &= aT_{S:R}(x) \\ T_{S:R}(x+y) &= T_{S:R}(x) + T_{S:R}(x) \\ N_{S:R}(1_S) &= 1_R \\ N_{S:R}(ax) &= a^n N_{S:R}(x) \\ N_{S:R}(xy) &= N_{S:R}(x) \cdot N_{S:R}(y) \end{aligned}$$

for any $x, y \in S$ and $a \in R$. Also x satisfies its own characteristic polynomial, that is $c_x(x) = 0$ and the norm and trace of x occur as the coefficients $c_x[0] = (-1)^n N_{S:R}(x)$ and $c_x[n-1] = -T_{S:R}(x)$ in the characteristic polynomial of x. A little less formal that is

$$c_x(t) = t^n - T_{S:R}(x)t^{n-1} + \cdots + (-1)^n N_{S:R}(x)$$

(8.40) Example:

(i) Consider the field extension $\mathbb{C} : \mathbb{R}$ in its standard ordered basis $(1, i)$. As $i \cdot 1 = 1$ and $i \cdot i = -1$ the matrix representation of λ_i is given to be the following

$$[\lambda_i] \;=\; \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

In particular we find $T_{\mathbb{C}:\mathbb{R}}(i) = 0$ and $N_{\mathbb{C}:\mathbb{R}}(i) = 1$, likewise $c_i(t) = t^2 + 1$. This is an example of the property $c_i(i) = 0$ and as $i \notin \mathbb{R}$ we can also conclude $\mu_i(t) = t^2 + 1$.

(ii) More generally: If $S : R$ is any ring extension and $x \in S$ is integral over R, then $R[x] : R$ is a finite ring extension. Suppose x has a minimal polynomial m_x, that is m_x is the monic generator of the null ideal $\mathfrak{v}_x = \mathsf{kn}(f \mapsto f(x)) = \{\, f \in R[t] \mid f(x) = 0 \,\}$. Then

$$R[t] \,\big/\, m_x R[t] \;\xrightarrow{\sim}\; R[x] \;:\; f + m_x R[t] \mapsto f(x)$$

is an isomorphism of R-algebras, by the first isomorphism theorem. Now by (8.10.(i)) $R[x] : R$ has the ordered basis $(1, x, \ldots, x^{n-1})$ where $n := \deg(m_x)$. As $\lambda_x(x^k) = x^{k+1}$ for any $k < n$ and x^n can be expressed, as $x^n = -m_x[0] - m_x[1]x - \cdots - m_x[n-1]x^{n-1}$ we find the following matrix representation of λ_x in this ordered basis:

$$[\lambda_x] \;=\; \begin{pmatrix} 0 & 0 & \cdots & 0 & -m_x[0] \\ 1 & 0 & \cdots & 0 & -m_x[1] \\ 0 & 1 & \cdots & 0 & -m_x[2] \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -m_x[n-1] \end{pmatrix} \;=\; \mathsf{comp}(m_x)$$

Both, the characteristic and minimal polynomials of this matrix are m_x again, according to (5.43), even for an arbitrary commutative ring R. Formally that is

$$c_{[\lambda_x]}(t) \;=\; m_{[\lambda_x]}(t) \;=\; m_x(t)$$

8.4 Algebraic Dependence

If E is a field and V an E-vector-space, then V is of the form $V = E^{\oplus B}$ where B is some basis of V over E. And this completely defines the algebraic structure of V. If A is an F-algebra, then it also is an E-vector-space, but $A = E^{\oplus B}$ doesn't help much, as the multiplicative structure of A is not respected - just look at $A = E[t]$ for a counter-example.
Therefore we need a different approach. The standard-algebra is a polynomial ring $R[t_i \mid i \in I]$, so the question is: How large a polynomial ring is contained in A? This is quite similar to the question: How large a free module $R^{\oplus I}$ is contained (in the R-module) M?
In (3.102.(viii)) we found a satisfactory answer to this question, in case R is an integral domain: There is a maximal linearly independent subset $L \subseteq M$ and any two of these share the same cardinality. This is what we called the *linear freedom* of M. So M contains an isomorphic copy of $F = R^{\oplus L}$ as a sub-module. However M can be larger still, but the rest M/F is a torsion module.
This is very similar to what we will find for R-algebras A, too. If A is an integral domain and the structural homomorphism $\alpha : a \mapsto a1_A$ is injective, then A contains an isomorphic copy of a polynomial ring $P = R[t_i \mid i \in I]$ and the maximal size $|I|$ of this is uniquely determined - it will be called *transcendence degree* of A over R. Again A may be larger, but the rest $A : P$ is an algebraic extension.

This is an astounding similarity, but the analogy is even more far-reaching: In case R is a PID and M is a finitely generated R-module, then (5.32) gives a detailed description of the structure M can have $M = R^f \oplus \text{TOR}(M)$ and we can even control the torsion-part very accurately. In case E is a field and A is a finitely generated E-algebra, then the Noetherian normalisation theorem will be the analogue for A: $A : P$ will be a finite extension, where P is an isomorphic copy of $E[t_1, \ldots, t_n]$ and we can even arrange P according to a given chain of ideals.
So let us begin with this beautiful theory: The first part is fairly easy, we will study algebraic ring extensions and prove that (in integral domains) algebraic dependence is a dependence relation again, such that we can reap the harvest of section 3.6 a second time. It also is easy to formulate the Noetherian normalisation theorem. Its proof, however, is one of those technical monsters, that dwell out there. In case you really want to work through it, you have been warned.

(8.41) Proposition: (viz. 1245)

(i) Let $S : R$ be a ring extension, such that $\text{NIL}(R) = 0$ (we say R is *reduced*). Then for any element $x \in S$ the following two statements are equivalent

 (a) x is algebraic over R

 (b) there is some $a \in R$ with $a \neq 0$ and ax is integral over R

(ii) Let $S : R$ be a ring extension, such that R is an integral domain, then the algebraic closure of R in S is an intermediate ring of $S : R$, that is

$$R\,1_S \quad \subseteq \quad \text{alg}(S : R) \quad \leq_{\text{a}} \quad S$$

(iii) Let $(S,+,\cdot)$ be an integral domain and $R \leq_r S$ be a sub-ring of S, then we get the equivalence of

(a) $S : R$ is algebraic

(b) $\text{QUOT}(S) : \text{QUOT}(R)$ is algebraic

And in this case we also get: Let us denote $U := R \setminus \{0\}$ such that $\text{QUOT}(R) = U^{-1}R$. Then we obtain a canonical isomorphism of the quotient field $\text{QUOT}(S)$ of S

$$U^{-1}S \xrightarrow{\sim} \text{QUOT}(S) \; : \; \frac{s}{u} \mapsto \frac{s}{u}$$

(iv) *Transitivity of being algebraic*: Let $(T,+,\cdot)$ be an integral domain and $S \leq_r T$ and $R \leq_r S$ be sub-rings of T. Then the following two statements are equivalent

(a) $T : R$ is algebraic

(b) $T : S$ and $S : T$ are algebraic

(v) *Artin-Tate-Lemma:* Let $T : R$ be a ring extensions and S be an intermediate ring $T : S : R$, such that (1) R in noetherian, (2) $T : R$ is finitely generated and (3) $T : S$ is finite. Then $S : R$ is finitely generated ring extension, too.

(8.42) Remark:
In (8.30.(vi)) we have seen, that the integral closure $\text{int}(S : R)$ of R in S is a ring again. If R is a field, then we have $\text{alg}(S : R) = \text{int}(S : R)$, such that the algebraic closure $\text{alg}(S : R)$ is a ring, as well. But we have just seen, that it suffices that R is an integral domain, for $\text{alg}(S : R)$ to be a ring, once more. However, for general R the algebraic closure need not be a sub-ring of S!

As an example let $R := \mathbb{Z}^2$ and $S := \mathbb{Z}[x]^2$. Then $(x,0) \in S$ is algebraic over R, as $(0,1) \cdot (x,0) = (0,0)$. Likewise $(0,x)$. However the sum $(x,0) + (0,x) = (x,x)$ is not algebraic over R as any polynomial $(f,g) \in R[t]$ turns (x,x) into $(f,g)(x,x) = (f(x),g(x))$ which only is zero, if both f and g are.

(8.43) Remark: (viz. 1257)
If $T : S$ and $S : R$ are ring extensions, such that $T : R$ is *integral* or *algebraic*, then $T : S$ and $S : R$ are integral resp. algebraic again (under reasonable assumptions). The same is true for *finite* (under quite strong assumptions). The converse implications are generally true. Also if $T : S$ and $S : R$ are *finitely generated*, say $T = S[y_1,\ldots,y_n]$ and $S = R[x_1,\ldots,x_m]$, then $T = R[x_1,\ldots,x_m,y_1,\ldots,y_n]$ such that $T : R$ is finitely generated again. The converse need not be true however: If $T : R$ is finitely generated, then $S : R$ need not be, even in extremely nice cases:

- Let $(R,+,\cdot)$ be a field and $B := E[x,y]$ the polynomial ring in two variables over E. Then we define A to be the sub-algebra of B generated by elements of the form xy^k where $k \in \mathbb{N}$. That is

$$A \; := \; E[xy^k \mid k \in \mathbb{N}]$$

- We then find $xx^kA \subseteq xy^kE + x^2y^kB$. Thereby we are able to construct ideals $\mathfrak{a}_k \trianglelefteq_\mathrm{i} A$ with the property $xx^{y+1} \notin \mathfrak{a}_k$. For these ideals we take

$$\mathfrak{a}_k \;:=\; \sum_{j=0}^{k} xy^jA$$

 Then it is clear that these ideals for an ascending chain and as $xy^{k+1} \notin \mathfrak{a}_k$ the inclusions of these chain even are strict: $\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \ldots \subset \mathfrak{a}_k \subset \ldots$.

- In particular A is not a noetherian ring. So it cannot be finitely generated: If it was then (as E is a field) the Hilbert basis theorem (2.42) would imply, that A is noetherian - which it is not. Thus there is an infinitely generated E-algebra A inside an E-algebra B, that is generated by 2 elements! This counter-example is sharp however, as we see in the proposition below.

- $(\diamondsuit)$ Clearly $\{ x, y \}$ is a transcendence basis of $B : E$. We also find a transcendence basis $\{ x, xy \}$ of $A : E$, so this does not contradict the properties of transcendence bases and the transcendence degree, that will be introduced in the next section.

- **Proposition:** Let $(E, +, \cdot)$ is a field and B be an E-algebra, that is generated by a single element, say $B = E[b]$ for some $b \in B$. If then $A \leq_\mathrm{a} B$ is a sub-algebra of B, then A is finitely generated.

(8.44) Definition:
Consider a ring extension $S : R$, (i.e. S is a commutative, unital R-algebra). Then for any element $x \in S$ and any subset $U \subseteq S$ we define the following notions

(i) Let us introduce a relation $\vdash$ between subsets $U \subseteq S$ and elements $x \in S$ of S: We say x is **algebraically dependent on** U, and write this as $U \vdash x$, iff there is a non-zero polynomial f over $R[U]$ such that $f(x) = 0$, formally that is

$$\exists f \in R[U][t] \;:\; f \neq 0 \;\text{ and }\; f(x) = 0$$

(ii) A finite subset $U = \{ u_1, \ldots, u_n \} \subseteq S$ is said to be **algebraically independent** iff for any polynomial $f \in R[t_1, \ldots, t_n]$ with the same number n of variables, we get the implication

$$f(u_1, \ldots, u_n) \;=\; 0 \quad\Longrightarrow\quad f \;=\; 0$$

 And an arbitrary subset $U \subseteq S$ is said to be **algebraically independent**, iff any finite subset of U is algebraically independent in the sense of finite sets. Of course U is said to be **algebraically dependent**, iff it is not algebraically independent.

(iii) Now a subset $U \subseteq S$ will be called a **transcendence basis** of S over R, iff it is algebraically independent and $S : R[U]$ is an algebraic extension (that is, iff any $x \in S$ satisfies $U \vdash x$).

(8.45) Lemma: (viz. 1247)
Let $S : R$ be a ring extension, such that S is an integral domain and the structural homomorphism $\alpha : a \mapsto a1_S$ is injective. Also let $x \in S$ be any element and $U \subseteq S$ be any subset of S, then the following statements are true

(i) The following four properties concerning U and x are equivalent

(a) $U \vdash x$

(b) $x \in \mathrm{alg}(S : R[U])$

(c) $ax \in \mathrm{int}(S : R[U])$, for some $a \in R$ with $a \neq 0$

(d) $R[U \cup \{ x \}] : R[U]$ is an algebraic ring extension

(ii) $\vdash$ is a dependence relation

(iii) If $U \subseteq S$ is algebraically independent, then the following two statements are equivalent:

(a) $U \vdash x$

(b) $U \cup \{ x \}$ is algebraic dependent (over R)

(iv) If $U = \{ u_1, \ldots, u_n \}$ is a finite set, then the following three statements are equivalent:

(a) $\{ u_1, \ldots, u_n \}$ is algebraically independent

(b) $\forall k \in 1 \ldots n$ we get $U \setminus \{ u_k \} \nvdash u_k$

(c) $\forall k \in 1 \ldots n$ we get $\{ u_1, \ldots, u_{k-1} \} \nvdash u_k$

(8.46) Corollary: (viz. 1250)
Let $S : R$ be a ring extension, such that S is an integral domain and the structural homomorphism $\alpha : a \mapsto a1_S$ is injective. Then the relation $\vdash$ of algebraic dependence is a dependence relation, by (8.45.(ii)) and therefore we get the following statements

(i) If $U \subseteq S$ is any subset, then the following three statements are equivalent

(a) U is $\vdash$independent

(b) U is algebraically independent

(c) $R[t_u \mid u \in U] \xrightarrow{\sim} R[U] : t_u \mapsto u$ is an isomorphism of R-algebras

(ii) For any subset $U \subseteq S$ we have $\langle U \rangle = \mathrm{alg}(S : R[U])$, in particular equivalent are

(a) U $\vdash$generates S

(b) $S : R[U]$ is an algebraic ring extension

(iii) If $U \subseteq S$ is any subset, then the following two statements are equivalent

(a) U is a $\vdash$basis of S

(b) U is a transcendence basis of $S : R$

(iv) *Basis Exchange Theorem:* Let V be a transcendence basis of $S : R$ and consider any subset $U \subseteq V$. Also let $U' \subseteq S$ be some subset, such that (1) U' is algebraically independent, (2) $R[U'] \subseteq R[U]$ is a sub-ring and (3) $R[U] : R[U']$ is an algebraic extension. Then also the following set

$$\big(V \setminus U\big) \cup U' \quad \text{is a transcendence basis of } S : R$$

(8.47) Remark:
Let $S : R$ be a ring extension, such that S is an integral domain and the structural homomorphism $\alpha : a \mapsto a1_S$ is injective. Then we can reap the harvest from (8.45.(ii)) and (8.46) by importing the properties of dependence relations for algebraic dependence. For convenience let us restate the major theorems in (3.57) in the language of algebraic dependence:

(i) If $U \subseteq S$ is algebraically independent and $W \subseteq S$ is a subset, such that $S : R[W]$ is algebraic, then there is some V with $U \subseteq V \subseteq W$, such that V is a transcendence basis of $S : R$. In particular any such ring extension $S : R$ has a transcendence basis.

(ii) If U and $V \subseteq S$ both are transcendence bases of $S : R$ then they are of the same cardinality $|U| = |V|$. This enables us to name the cardinality of any (and hence all) transcendence basis of $S : R$ the **transcendence degree** of $S : R$

$$\operatorname{trdeg}(S : R) \;:=\; |U|$$

(iii) If $U \subseteq S$ is any subset, then we get: (1) If U is algebraically independent, then $|U| \leq \operatorname{trdeg}(S : R)$ and (2) if $S : R[U]$ is algebraic, then $|U| \geq \operatorname{trdeg}(S : R)$.

(iv) If $U \subseteq S$ is a transcendence basis of $S : R$, such that $\operatorname{trdeg}(S : R) = |U| < \infty$ is finite and $V \subseteq S$ is another algebraically independent set in S, then we have the equivalence of

(a) $|V| = \operatorname{trdeg}(S : R)$

(b) V is a transcendence basis of $S : R$

(8.48) Example: (viz. 1251)

(i) If $S : R$ is an algebraic extension then $\emptyset \subseteq S$ is a transcendence basis of $S : R$ [$\emptyset$ is algebraically independent and $R[\emptyset]$]. The converse is true as well and hence we have

$$\operatorname{trdeg}(S : R) \;=\; 0 \quad\Longleftrightarrow\quad S : R \text{ is algebraic}$$

(ii) If $(R, +, \cdot)$ is an integral domain and $S = R[t_i \mid i \in I]$ is a polynomial ring over R, then the set $T := \{\, t_i \mid i \in I \,\}$ clearly is a transcendence basis of $S : R$, we even have $S = R[T]$. In particular

$$\operatorname{trdeg}\big(R[t_i \mid i \in I] : R\big) \;=\; |I|$$

(iii) If $(R, +, \cdot)$ is an integral domain and $E := \operatorname{QUOT}(R)$ its quotient field, then $E : R$ is an algebraic extension, as any $a/b \in E$ satisfies a polynomial $bt - a \in R[t]$ of degree 1. Therefore

$$\operatorname{trdeg}\big(\operatorname{QUOT}(R) : R\big) \;=\; 0$$

(iv) A special case of (8.49.(i)) below is the field of rational functions $F = E(t_1, \ldots, t_n)$ over a field $(E, +, \cdot)$. This is the quotient field of of the polynomial ring $E[t_1, \ldots, t_n]$. We then find, that the set $\{\, t_1, \ldots, t_n \,\} \subseteq F$ is a transcendence basis of $F : E$, as well.

(v) Let $(R,+,\cdot)$ be an integral domain and $S = R[t_1,\ldots,t_n]$ be the polynomial ring, in finitely many variables. By (ii) $\{\, t_1,\ldots,t_n \,\}$ is a transcendence basis of $S : R$. Let $s_1,\ldots,s_n \in S$ be the symmetric polynomials in n variables. Then by (7.67.(iii)) $\{\, s_1,\ldots,s_n \,\}$ is algebraically independent, too. Now (8.47.(iv)) tells us, that $\{\, s_1,\ldots,s_n \,\}$ is a transcendence basis of S, too. That is

$$R[t_1,\ldots,t_n] : R[s_1,\ldots,s_n] \text{ is algebraic}$$

Note that the algebra of symmetric polynomials $R[s_1,\ldots,s_n]$ is smaller than the polynomial ring $R[t_1,\ldots,t_n]$ itself, but the transcendence degrees over R are equal.

(vi) Let $(R,+,\cdot)$ be an integral domain and $A := R[t_1,\ldots,t_n]$ be the polynomial ring in n variables. If now $p \in A$ is a prime polynomial, with $\deg_1(p) \geq 1$, then we take

$$S \;:=\; {}^{A}\Big/_{p\,A}$$

for the extension ring of R. Now define $u_k := t_k + fA \in S$ and $U := \{\, u_2,\ldots,u_n \,\}$, then U is a transcendence basis of $S : R$ and in particular we have

$$\operatorname{trdeg}(S : R) \;=\; n-1$$

(vii) Let $(S,+,\cdot)$ be an integral domain, $R \leq_{\mathrm{r}} S$ be a sub-ring and $U \subseteq S$ be a transcendence basis of $S : R$. For any $u \in U$ pick up a power $1 \leq m(u) \in \mathbb{N}$. Then the set $U' := \left\{\, u^{m(u)} \mid u \in U \,\right\}$ is a transcendence basis of $S : R$, as well.

(8.49) Proposition: (viz. 1252)
Let $(S,+,\cdot)$ be an integral domain and $R \leq_{\mathrm{r}} S$ and $Q \leq_{\mathrm{r}} R$ be sub-rings of S. Then the following three statements are true

(i) Let $1 \leq n \in \mathbb{N}$ and $V = \{\, v_1,\ldots,v_n \,\} \subseteq S$ be a transcendence basis of $S : R$ $n \geq 1$) and $A = (a_{i,j}) \in \operatorname{mat}_n(R)$ be an $(n \times n)$-matrix. For any $i \in 1\ldots n$ define $w_i = [Au]_i = \sum_j a_{i,j}u_i$. Then the following two statements are equivalent

(a) $\det(A) = 0$

(b) $\{\, w_1,\ldots,w_n \,\}$ is a transcendence basis of $S : R$

(ii) If $V \subseteq S$ is a transcendence basis of $S : R$, then $V/1 := \{\, v/1 \mid v \in V \,\} \subseteq F$ is a transcendence basis of the extension of the quotient fields $\textsc{quot}(S) : \textsc{quot}(R)$ and therefore we have

$$\operatorname{trdeg}\big(\textsc{quot}(S) : \textsc{quot}(R)\big) \;=\; \operatorname{trdeg}\big(S : R\big)$$

(iii) If $U \subseteq R$ is a transcendence basis of $R : Q$ and $V \subseteq S$ is a transcendence basis of $S : R$ again, then $U \cap V = \emptyset$ and $U \cup V$ is a transcendence basis of $S : Q$. In particular we have

$$\operatorname{trdeg}\big(S : Q\big) \;=\; \operatorname{trdeg}\big(S : R\big) + \operatorname{trdeg}\big(R : Q\big)$$

(8.50) Remark: (viz. 1254)
In the above we always required S to be an integral domain. This is due to the fact, that we needed the transitivity of algebraic extensions and that the algebraic closure is a sub-ring again - refer to (8.41). This is not needed with *integral* instead of *algebraic*. So the above statements can often be modified, in case $S : R[U]$ is integral. And sometimes S being integral is not needed at all. Here are a few examples of such statements:

(i) If $S : R$ is any ring extension, then a subset $U = \{ u_1, \ldots, u_n \} \subseteq S$ is algebraically independent, if and only if the evaluation homomorphism $\varepsilon : R[t_1, \ldots, t_n] \twoheadrightarrow R[U] : f \mapsto f(u_1, \ldots, u_n)$ is an isomorphism of R-algebras.

Nota that this has far-reaching consequences: If R is an integral domain, then the polynomial ring $R[t_1, \ldots, t_n]$ is an integral domain, too (7.12.(vii)). Hence $R[U]$ is an integral domain, due to the isomorphy in (i). Likewise, if R is noetherian and U is finite, then $R[U]$ is noetherian again (2.42). Finally, if R is an UFD, then $R[U]$ inherits being an UFD, as well (7.29.(viii)).

(ii) Let $S : R$ be any ring extension and let $U, V \subseteq S$ such that U is an algebraically independent set. Then the following two statements are equivalent

 (a) $U \cup V$ is algebraically dependent over R

 (b) There is some $v \in V$ such that v is algebraically dependent over $R[U \cup V \setminus \{ v \}]$.

(iii) If $S : R$ is any ring extension and $U \subseteq S$ is algebraically independent over R, then there is some subset $U^* \subseteq S$, such that (1) $U \subseteq U^*$, (2) U^* is algebraically independent over R, too and (3) $S : R[U^*]$ is an algebraic extension of rings.

(iv) Let $S : R$ be any ring extension and $V \subseteq S$ be a subset, such that $S : R[V]$ is integral. Also let $U \subseteq V$ and $U' \subseteq S$ be subsets, such that (1) $R[U'] \subseteq R[U]$ and (2) $R[U] : R[U']$ is integral. Then $S : R[V']$ is integral, too, where $V' := (V \setminus U) \cup U'$.

(v) Let $S : R$ be any ring extension and $V \subseteq S$ be algebraically independent set. Also let $U \subseteq V$ and $U' \subseteq S$ be subsets, such that (1) U' is algebraically independent and (2) $R[U'] \subseteq R[U]$ Then $V' := (V \setminus U) \cup U'$ is algebraically independent, too.

Noetherian Normalisation
We will now aim for the Noetherian normalisation theorem, the structure theorem for finitely generated, commutative algebras A over a field E. It refines the theory of transcendence bases in two ways, as it contains the existence of an algebraically independent set $\{ z_1, \ldots, z_n \} \subseteq A$ (1) even if A is not an integral domain and (2) such that for $P = E[z_1, \ldots, z_n]$ the extension $A : P$ is finite, not only algebraic. It will be crucial for dimension theory, e.g. when proving that in (a finitely generated algebra A, that also is an integral domain) all maximal chain of prime ideals have the same length.
In order to put the proof into a readable form we chose to export a special case, as a separate proposition. Of course we already know, that a non-zero polynomial $0 \neq g \in E[t_1, \ldots, t_n]$ can be appended to a transcendence basis $\{ g, z_2, \ldots, z_n \}$, as this is a property of dependence relations. The proposition however is computational and will be the staging area to get $A : P$ finite.

(8.51) Proposition: (viz. 1261)
Let $(E,+,\cdot)$ be a field and consider $A := E[t_1,\ldots,t_n]$ a polynomial ring in $n \geq 1$ variables. If now $g \in A$ is a polynomial with, with $\deg(g) \geq 1$, then there are some $1 \leq m_2,\ldots,m_n \in \mathbb{N}$ such that for $z_i := t_i - t_1^{m_i} \in A$ (where $i \in 2\ldots n$) and $P := E[g,z_2,\ldots,z_n]$ we get

(1) $\{ g,z_2,\ldots,z_n \} \subseteq A$ is algebraically independent

(2) $A : P$ is a finite ring-extension, where $P := E[g,z_2,\ldots,z_n]$

(3) The ideal gP is prime in P and satisfies $gA \cap P = gP$

Nota In case $n = 1$ we do not need z_2 to z_n and the statements reduce to (1) g is not algebraic over E [which is clear, as $\deg(f(g)) = \deg(f) \cdot \deg(g)$], (2) $A : E[g]$ is a finite ring-extension [which is clear, as t_1 is algebraic over P, as $g(t_1) - g = 0$] and (3) gP is prime in P and $gA \cap P = gP$ [this has to be proved].

Nota The proof relies on (7.57) to get the z_i. If E is an infinite field, then the same proposition tells us, that we could have chosen the z_i in another way, too: There are non-zero $0 \neq a_2,\ldots,a_n \in E$, such that $z_i = t_i - a_i t_1$ the $\{ g,z_2,\ldots,z_n \}$ is another algebraically independent set satisfying properties (1) to (3).

(8.52) Theorem: (viz. 1263)
Noetherian Normalisation Theorem: Let $(E,+,\cdot)$ be a field and $A \neq 0$ be a finitely generated E-algebra. Also consider a chain $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \ldots \subseteq \mathfrak{a}_r \trianglelefteq_{\mathrm{i}} A$ of proper ideals in A, that is $\mathfrak{a}_r \neq A$, of length $r \in \mathbb{N}$. Then there are elements $z_1,\ldots,z_n \in A$ and numbers $0 \leq k(1) \leq k(2) \leq \cdots \leq k(r) \leq n$ such that

(1) $\{ z_1,\ldots,z_n \} \subseteq A$ is algebraically independent

(2) $A : P$ is a finite ring-extension, where $P := E[z_1,\ldots,z_n]$

(3) For any $i \in 1\ldots r$ we have $\mathfrak{a}_i \cap P = z_1 P + \cdots + z_{k(i)} P$

Nota By (8.30.(v)) the ring-extension $A : P$ also is integral and hence algebraic. Therefore due to (1) and (2) $\{ z_1,\ldots,z_n \}$ is a transcendence basis of $A : E$. In case A also is an integral domain, this means that n is fixed to be $n = \mathrm{trdeg}(A : E)$ because of (8.47.(ii)).

Nota Under these assumptions A is a noetherian ring, by the Hilbert basis theorem (2.42). And because of (1) P is isomorphic to a polynomial ring in n variables over a field, by (8.50.(i)). In particular P is a noetherian UFD and therefore A also is a noetherian P-module, as we have (2) and (3.111.(vi)).

Nota As $\{ z_1,\ldots,z_n \}$ is algebraically independent, P is isomorphic to a polynomial ring $E[t_1,\ldots,t_n]$. Thereby $\mathfrak{a}_i \cap P$ corresponds to the ideal $\langle t_1,\ldots,t_{k(i)} \rangle_{\mathrm{i}} \trianglelefteq_{\mathrm{i}} E[t_1,\ldots,t_n]$ and therefore is prime in P

$$\{ \mathfrak{a}_i \cap P \mid i \in 1\ldots r \} \quad \subseteq \quad \mathrm{Spec}(P)$$

Nota This theorem will be continued in (8.76.(iii)). There we will prove that the numbers n and (in case A is an integral domain) $k(i)$ are uniquely determined to be $n = \mathrm{kdim}(A)$ and $k(i) = \mathrm{height}(\mathfrak{a}_i)$.

8.5 Algebraically closed Fields

In this section we will study field extensions and algebraically closed fields. The latter are a very rare but incredibly powerful fields in which any non-constant polynomial always has all its roots. As such these fields can no longer be extended algebraically, a true extension has to be transcendental. While few fields are algebraically closed, to begin with, any field admits an algebraic extension that is algebraically closed. E.g. the reals $\mathbb{R}$ are contained in the algebraically closed field $\mathbb{C}$ of complex numbers.
One of the major benefits of algebraically closed fields F is that any point of F^n corresponds to a maximal ideal of the polynomial ring $F[t_1,\dots,t_n]$. This has far reaching consequences: From this we find that algebraic sets (which are objects of geometry) correspond to radical ideals of $F[t_1,\dots,t_n]$ (which are objects of algebra). This gives birth to the entirely new branch of algebraic geometry, which studies geometric objects through the looking glass of its algebraic counterparts. These correspondences will all be formulated and proved in this section.

(8.53) Definition:
Recall that we speak of a ring extension $F : E$, if F is a unital E-algebra. We now define a **field extension** $F : E$ to be a ring extension, such that both, E and F, are fields. In this case a subset $P \subseteq F$ is said to be an **intermediate field** of $F : E$ - which we denote by $F : P : E$ - iff P is a subalgebra and a subfield of F. That is $P \leq_r F$ is a subring of F that also satisfies the properties

(1) for any $p \in P$ with $p \neq 0$ we get $p^{-1} \in P$

(2) for any $a \in E$ and any $p \in P$ we get $ap \in P$

In a field extension $F : E$ clearly F is an E-vector space (and in particular a torsion free E-module). Therefore the structural homomorphism $\alpha : E \hookrightarrow F : a \mapsto a1_F$ is injective and its image $\mathrm{im}(\alpha) = E\,1_F$ is an intermediate field of $F : E$

$$E\,1_F \;=\; \{\, a1_F \mid a \in E \,\}$$

Prob If $a1_F = b1_F$ we have $d1_F = 0_F$ for $d := a - b$. If we had $d \neq 0$, then $1_E = d^{-1}d$ such that $1_F = 1_E1_F = d^{-1}d1_F = d^{-1}0_F = 0_F$, which contradicts $F \neq 0$. Thus we have $a = b$, which is the injectivity of α. As α is a homomorphism of E-algebras, its image $E\,1_F$ is a subalgebra of F. Also, as $a1_F \neq 0_F$ implies $a \neq 0_E$ we get $(a1_F)^{-1} = a^{-1}1_F \in E\,1_F$, such that $E\,1_F$ also is a subfield of F.

(8.54) Remark:
If $F : E$ is a field extension and $U \subseteq F$ is a subset, then by (1.52) there is a sub-field $E \cup U$. We denote this intermediate field of $F : E$, that is generated by U by the symbol

$$E(U) \;:=\; \langle E \cup U \rangle_f \quad \leq_f \quad F$$

By (1.55) the intermediate field generated by U consists precisely of the quotients $f/g := fg^{-1}$ of elements $f, g \in E[U]$ of the intermediate ring generated by U. Yet by (8.4) the intermediate ring $E[U]$ consists of all polynomial expressions in finitely many elements of U over E. So combining these results we get an explicit description of $E(U)$ to be

$$E(U) \;=\; \left\{ fg^{-1} \mid f,g \in E[U],\, g \neq 0 \right\}$$

$$= \left\{ \frac{f(u_1,\ldots,u_n)}{g(u_1,\ldots,u_n)} \;\middle|\; \begin{array}{l} 1 \leq n \in \mathbb{N}, u_1,\ldots,u_n \in U \\ f,g \in R[t_1,\ldots,t_n], \\ g(u_1,\ldots,u_n) \neq 0 \end{array} \right\}$$

(8.55) Definition: (viz. 1268)
Let $(F,+,\cdot)$ be a field, then F is said to be **algebraically closed**, iff it satisfies one (and hence all) of the following six equivalent properties

(a) If $K:F$ is any field extension, then $\mathrm{alg}(K:F) = F1_K$.

(b) If K is a field such that $K:F$ is an algebraic field extension, then $K = F1_K$.

(c) If K is a field such that $K:F$ is a finite field extension, then $K = F1_K$.

(d) Any non-constant polynomial splits into linear factors over F. That is for any $f \in F[t]$ of degree $n := \deg(f) \geq 1$, there are some $a \in F$ and $x_1,\ldots,x_n \in F$ such that we get the following identity

$$f \;=\; a\prod_{i=1}^{n}(t-x_i)$$

(e) Any non-constant polynomial over F has a root in F, that is: If $f \in F[t]$ is of $\deg(f) \geq 1$, then there is some $x \in F$, such that $f(x) = 0$.

(f) If $p \in F[t]$ is an irreducible polynomial, then $\deg(p) = 1$

By (7.79.(iii)) the field $\mathbb{C}$ of complex numbers is algebraically closed. But the proof is analytic in nature and relies on the fact that every real polynomial of odd degree has a root. Also it is rather intricate and for this reason we will give an alternate proof in section 8.6. What we aim for next, is to prove that any field E is contained in an algebraically closed field. In fact this field uniquely determined (up to isomorphy) and hence called the *algebraic closure* of E. The following corollary will be vastly generalized in (8.59.(iii)), but only by using much more powerful tools.

(8.56) Corollary: (viz. 1269)
In any field $(F,+,\cdot)$ the maximal ideals of the polynomial ring $F[t]$ are precisely the principal ideals induces by irreducible polynomials. Formally this is the identity

$$\mathrm{Smax}\big(F[t]\big) \;= \{\, pF[t] \mid p \in F[t] \text{ irreducible} \,\}$$

Hence, if F is algebraically closed, then the maximal ideals of $F[t]$ are precisely the principal ideals induced by polynomials of the form $t-a \in F[t]$ for some $a \in F$. Formally again

$$\mathrm{Smax}\big(F[t]\big) \;= \{\, (t-a)F[t] \mid a \in F \,\}$$

Lemma von Steinitz: Konstruktion des algebraischen Abschlusses

(8.57) Proposition: (viz. 1269)

(i) If $(R,+,\cdot)$ is any commutative ring and $(A,+)$ is any monoid, then the cardinality of the polynomial ring $R[t \mid A]$ is the maximal cardinality of R and A. Formally that is

$$|R[t \mid A]| \;=\; \max\{\,|R|, |A|\,\}$$

(ii) If $(R,+,\cdot)$ is any commutative ring and $I \neq \emptyset$ is any non-empty set, then the cardinality of polynomial ring $R[t_i \mid i \in I]$ is given to be the maximal cardinality if $\mathbb{N}$, A and R:

$$|R[t_i \mid i \in I]| \;=\; \max\{\,|\mathbb{N}|, |R|, |I|\,\}$$

NOTA The main task here lies in proving $|\mathbb{N}^{\oplus I}| = \max\{\,|\mathbb{N}|, |I|\,\}$, the rest is then clear by (i). Though this is generally true, we did not formulate this identity as a separate proposition.

(iii) Let $S : R$ be an algebraic ring extension in which $(S,+,\cdot)$ is an integral domain. Then the cardinality of S cannot exceed that of $\mathbb{N}$ and R, since

$$|S| \;\leq\; \max\{\,|\mathbb{N}|, |R|\,\}$$

(iv) If $(E,+,\cdot)$ is any field, $P := \text{PRF}(E)$ its prime field and $F := \text{AC}(E)$ its algebraic closure. Then we have the following identity for the transcendence degree of $F : P$

$$|F| \;=\; \max\{\,|\mathbb{N}|, \text{trdeg}(F : P)\,\}$$

(v) If $(R,+,\cdot)$ is a commutative noetherian ring, $I \neq \emptyset$ is any non-empty set and $\mathfrak{a} \trianglelefteq_{\text{i}} R[t_i \mid i \in I]$ is an ideal in the polynomial ring, then we get: (1) If I is finite, then there is a finite subset $A \subseteq R[t_i \mid i \in I]$ such that $\mathfrak{a} = \langle A\rangle_{\text{i}}$. And (2) if I is infinite, then there is a subset $A \subseteq R[t_i \mid i \in I]$ such that $\mathfrak{a} = \langle A\rangle_{\text{i}}$ and $|A| \leq |I|$.

Hilbert's Nullstellensatz

Fix any commutative ring $(R,+,\cdot)$, a non-empty index set I and let $A := R[t_i \mid i \in I]$ be the polynomial ring $R[\mathbb{N}^{\oplus I}]$ over R in the variables t_i where $i \in I$. Recall that the evaluation $f(x)$ of a polynomial $f \in A$ in a point $x = (x_i) \in R^I$ - introduced in (7.52) - is well-defined. By construction A is a commutative R-algebra and the set $\text{ahom}(A,R)$ of R-algebra homomorphisms from A to R becomes a commutative algebra under the point-wise operations of functions from A to R. As $\varepsilon_x : f \mapsto f(x)$ is a homomorphism of R-algebras, we obtain a map from R^I to $\text{ahom}(A,R)$ by virtue of

$$R^I \;\to\; \text{ahom}(A,R) \;:\; x \;\mapsto\; \varepsilon_x$$

$$\varepsilon_x \;:\; A \to R \;:\; f \;\mapsto\; f(x)$$

And thereby the kernel $\mathfrak{m}_x := \text{kn}(\varepsilon_x) \trianglelefteq_{\text{i}} A$ is an ideal in A and if R is a field, it even is a maximal ideal of A. As in (7.60), for any subset $X \subseteq R^I$, we define the the *vanishing ideal* $\mathbb{I}(X)$ of X to be the set of all polynomials whose zero-locus contains X, that is

$$\mathbb{I}(X) \;:=\; \{\, f \in A \mid \forall\, x \in X : f(x) = 0\,\} \;=\; \bigcap_{x \in X} \mathfrak{m}_x$$

Likewise for a set $P \subseteq A$ of polynomials we denote the *algebraic set* $\mathbb{V}(P)$ of P to consist of those points, that belong to the zero locus of all the polynomials of P, that is

$$\mathbb{V}(P) := \left\{ x \in R^I \mid \forall f \in P : f(x) = 0 \right\} = \bigcap_{f \in P} \mathbb{V}(f)$$

We have seen in (7.62) that for an integral domain R the algebraic sets form the closed sets $\mathcal{Z}(R^I) = \{ \mathbb{V}(P) \mid P \subseteq A \}$ of the so-called *Zariski-topology* on R^I. Also the maps $\mathbb{I}$ and $\mathbb{V}$ thereby form a contra-variant Galois connection between the set of ideals of A and algebraic sets of R^I

$$\begin{array}{rcl} \{ \mathfrak{a} \mid \mathfrak{a} \trianglelefteq_{\mathrm{i}} A \} & \to & \left\{ X \mid X \subseteq R^I \right\} \\ \mathfrak{a} & \mapsto & \mathbb{V}(\mathfrak{a}) \\ \mathbb{I}(X) & \leftarrow\!\shortmid & X \end{array}$$

That is to say (1) for any $X \subseteq Y \subseteq R^I$ we get $\mathbb{I}(Y) \subseteq \mathbb{I}(X)$, (2) for any $\mathfrak{a}, \mathfrak{b} \trianglelefteq_{\mathrm{i}} A$ with $\mathfrak{a} \subseteq \mathfrak{b}$ we get $\mathbb{V}(\mathfrak{b}) \subseteq \mathbb{V}(\mathfrak{a})$, (3) for any $\mathfrak{a} \trianglelefteq_{\mathrm{i}} A$ we get $\mathfrak{a} \subseteq \mathbb{IV}(\mathfrak{a})$ and (4) for any $X \subseteq R^I$ we get $X \subseteq \mathbb{VI}(X)$. In this case we also have (5) $\mathbb{V}(P) = \mathbb{V}(\mathfrak{a})$ for any $P \subseteq A$, where we let $\mathfrak{a} := \langle P \rangle_{\mathrm{i}}$. As always with a Galois connection, we get $\mathbb{IVI} = \mathbb{I}$ and $\mathbb{VIV} = \mathbb{V}$ resulting in a one-to-one correspondence of the form

$$\begin{array}{rcl} \left\{ \mathbb{I}(X) \mid X \subseteq R^I \right\} & \longleftrightarrow & \{ \mathbb{V}(\mathfrak{a}) \mid \mathfrak{a} \trianglelefteq_{\mathrm{i}} A \} \\ \mathfrak{a} & \mapsto & \mathbb{V}(\mathfrak{a}) \\ \mathbb{I}(X) & \leftarrow\!\shortmid & X \end{array}$$

For a ring R with $\mathrm{NIL}(R) = 0$ the vanishing ideals $\mathbb{I}(X)$ are radical ideals, $\mathbb{I}(X) \in \mathrm{Srad}(A)$, but in general not every radical ideal occures as a vanishing ideal of some algebraic set $X \subseteq R^I$. It is not entirely satisfactory to not have a criterion for whether an ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} A$ is of the form $\mathfrak{a} = \mathbb{I}(X)$ for some $X \in \mathcal{Z}(R^I)$ and the Hilbert's Nullstellensatz is precisely the answer to this question: If R is an algebraically closed field satisfying $|I| < |R|$, then any radical ideal is the vanishing ideal of some $X \subseteq R^I$. If R is flawed, in one way or the other, there will be radical (even maximal) ideals not corresponding to an algebraic set. This will be the topic of corollary (8.62).

(8.58) Proposition: (viz. 599)
Let $(R, +, \cdot)$ be any non-zero, commutative ring, I be a non-empty index set and abbreviate the polynomial algebra $A := R[t_i \mid i \in I]$. Then we get the following statements

(i) If $\mathfrak{a} \trianglelefteq_{\mathrm{i}} A$ is a proper ideal (i.e. $\mathfrak{a} \neq A$) and φ is an R-algebra homomorphism φ of the following form, then for any $a \in R$ we get $\varphi(a1_A + \mathfrak{a}) = a$. In particular φ is non-zero and surjective:

$$\varphi : A \Big/ \mathfrak{a} \to R$$

(ii) Suppose that *for any* proper ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} A$ there is an R-algebra homomorphism φ of the following form, then R already has to be an algebraically closed field:

$$\varphi : A \Big/ \mathfrak{a} \to R$$

(iii) For any point $x = (x_i) \in R^I$ the ideal $\mathfrak{m}_x := \langle t_i - x_i \mid i \in I \rangle_{\mathfrak{i}}$ of A admits the one and only solution x and thereby $\mathfrak{m}_x$ is the kernel of the evaluation homomorphism $\varepsilon_x : A \to R : f \mapsto f(x)$:

$$\mathbb{V}(\mathfrak{m}_x) \;=\; \{\, x \,\} \quad \text{and} \quad \mathbb{I}(x) \;=\; \mathfrak{m}_x$$

(iv) If R is a reduced ring (that is $\text{NIL}(R) = 0$), then for any ideal $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} A$ of A the radical ideal of $\mathfrak{a}$ is contained in the vanishing ideal of the algebraic set of $\mathfrak{a}$. Formally that is

$$\sqrt{\mathfrak{a}} \quad \subseteq \quad \mathbb{IV}(\mathfrak{a})$$

(8.59) Proposition: (viz. 601)
Similarly to the above, let $(F, +, \cdot)$ be a field, I be a non-empty index set and abbreviate the polynomial algebra $A := F[t_i \mid i \in I]$. Then we get the following statements

(i) If $x \in F^I$ is any point, then the ideal $\mathfrak{m}_x := \text{kn}(\varepsilon_x) = \langle t_i - x_i \mid i \in I \rangle_{\mathfrak{i}}$ is a maximal ideal of A and the following map is well-defined and injective

$$F^I \;\hookrightarrow\; \text{Smax}(A) \;:\; x \mapsto \mathfrak{m}_x$$

Definition: We say that A is **geometric**, iff this map even is surjective. That is iff every maximal ideal $\mathfrak{m} \in \text{Smax}(A)$ of A is of the form $\mathfrak{m} = \mathfrak{m}_x$ for some $x \in F^I$.

(ii) If A is geometric and $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} A$ is any proper ideal, then we obtain one-to-one correspondences between the algebraic set $\mathbb{V}(\mathfrak{a})$, the maximal ideals of $A/\mathfrak{a}$ and the algebra-homomorphisms from of $A/\mathfrak{a}$ to F, of the form

$$\begin{array}{ccccc} \mathbb{V}(\mathfrak{a}) & \longleftrightarrow & \text{Smax}\left(A \big/ \mathfrak{a}\right) & \longleftrightarrow & \text{ahom}\left(A \big/ \mathfrak{a}, F\right) \\ x & \mapsto & \mathfrak{m}_x \big/ \mathfrak{a} & \mapsto & \varepsilon_x : f + \mathfrak{a} \mapsto f(x) \\ & & \text{kn}(\varphi) & \mapsfrom & \varphi \end{array}$$

(iii) If I is finite and F is an algebraically closed field, then A is geometric.

(iv) If I is infinite, then A is geometric if and only if the polynomial ring $A[s]$ is geometric.

(8.60) Theorem: (viz. 604)
Let $(F, +, \cdot)$ be any non-zero, commutative ring, I be a non-empty index set and abbreviate the polynomial algebra $A := F[t_i \mid i \in I]$. Then the following nine statements (a) to (i) are equivalent

(a) F is an algebraically closed field and $|I| < |F|$.

(b) For any proper ideal $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} A$ there is an F-algebra homomorphism φ of the form

$$\varphi \;:\; A \big/ \mathfrak{a} \to F$$

(c) For any maximal ideal $\mathfrak{m} \trianglelefteq_{\mathfrak{i}} A$ there is an F-algebra homomorphism φ of the form

$$\varphi \;:\; A \big/ \mathfrak{m} \to F$$

(d) For any maximal ideal $\mathfrak{m} \trianglelefteq_{\mathrm{i}} A$ there is a point $x \in F^I$ such that $\mathfrak{m} = \mathfrak{m}_x$.

(e) The points of F^I correspond to the maximal ideals of A, under the following bijection

$$F^I \longleftrightarrow \mathrm{Smax}(A) \ : \ x \mapsto \mathfrak{m}_x$$

(f) For any maximal ideal $\mathfrak{m} \trianglelefteq_{\mathrm{i}} A$ and any finite subset $\Omega \subseteq I$ there is a tuple $a \in F^{\Omega}$ such that $\mathfrak{m} \cap F[t_i \mid i \in \Omega]$ is an ideal of the form

$$\mathfrak{m} \cap F[t_i \mid i \in \Omega] \ = \ \langle t_i - a_i \mid i \in \Omega \rangle_{\mathrm{i}} \ \trianglelefteq_{\mathrm{i}} \ F[t_i \mid i \in \Omega]$$

(g) F is a field and for any ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} A$ we get $\mathbb{V}(\mathfrak{a}) = \emptyset$ if and only if $\mathfrak{a} = A$.

(h) F is a field and if $K : F$ is any field extension and $U = \{ u_i \mid i \in I \} \subseteq K$ is a subset, such that $F[U]$ is a field, then there is an isomorphism of F-algebras, of the form

$$F[U] \ \xrightarrow{\sim} \ F$$

(i) For any ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} A$ the vanishing ideal of the algebraic set $\mathbb{V}(\mathfrak{a}) \subseteq F^I$ coincides with the radical ideal of $\mathfrak{a}$. Formally that is the identity

$$\sqrt{\mathfrak{a}} \ = \ \mathbb{IV}(\mathfrak{a})$$

Nota Item (f) might be a little misleading: In case $\Omega = \emptyset$ the assumption reads as: For any maximal ideal $\mathfrak{m} \trianglelefteq_{\mathrm{i}} A$ we get $\mathfrak{m} \cap F = 0$. But this property is equivalent to F being a field. Thus more explicitly we could reformulate (f) as: F is a field and for any maximal ideal $\mathfrak{m} \trianglelefteq_{\mathrm{i}} A$ and any *non-empty*, finite subset $\Omega \subseteq I$ we get the identity $\mathfrak{m} \cap F[t_i \mid i \in \Omega] = \langle t_i - a_i \mid i \in \Omega \rangle_{\mathrm{i}}$.

(8.61) Remark:
In 1952 S. Lang proved a similar equivalence: If F is an algebraically closed field and $P := \mathrm{PRF}(F)$ is the prime field of F, then property (d) holds true if and only if I is finite or $|I| < \mathrm{trdeg}(F : P)$. This is much the same as (a), since the transcendence degree satisfies

$$|F| \ = \ \max\{ \, |\mathbb{N}|, \mathrm{trdeg}(F : P) \, \}$$

(8.62) Corollary: (viz. 610)
If F is an algebraically closed field and I is a non-empty index set, such that $|I| < |F|$, then the algebraic subsets of F^I are in 1-to-1 correspondence with the radical ideals of the polynomial algebra $A := F[t_i \mid i \in I]$. That is, if we abbreviate

$$\begin{aligned} \mathrm{Srad}(A) \ &= \ \left\{ \mathfrak{a} \trianglelefteq_{\mathrm{i}} A \mid \sqrt{\mathfrak{a}} = \mathfrak{a} \right\} \\ \mathcal{Z}(F^I) \ &= \ \{ \, \mathbb{V}(\mathfrak{a}) \mid \mathfrak{a} \trianglelefteq_{\mathrm{i}} A \, \} \end{aligned}$$

then $\mathbb{V} : \mathrm{Srad}(A) \to \mathcal{Z}(F^I)$ and $\mathbb{I} : \mathcal{Z}(F^I) \to \mathrm{Srad}(A)$ are well-defined, mutually inverse maps: $\mathbb{I} = \mathbb{V}^{-1}$. If F is not algebraically closed or $|F| \leq |I|$, then $\mathbb{VI} = \mathbb{1}$ is still satisfied, but $\mathbb{IV} = \mathbb{1}$ (and

hence the correspondence) fails.

(8.63) Corollary: (viz. 610)
Let R be any commutative ring and $I \subseteq J$ be index sets, such that I is non-empty. Then we abbreviate the polynomial rings $R[I] := R[t_i \mid i \in I]$ and likewise $R[J] := R[t_j \mid j \in J]$. Let us denote the canonical projection from R^J onto R^I by π_I^J below, then we get

$$\pi_I^J \;:\; R^J \;\twoheadrightarrow\; R^I \;:\; (x_j)_{j\in J} \;\mapsto\; (x_i)_{i\in I}$$

(i) Let $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R[I]$ be an ideal in the polynomial sub-ring $R[I] \leq R[J]$, then the set of the pushed-out ideal $\mathfrak{a}R[J]$ is just the pull-back of the algebraic set of $\mathfrak{a}$, that is

$$\mathbb{V}\big(\mathfrak{a}\,R[J]\big) \;\;=\;\; \big(\pi_I^J\big)^{-1}\big(\mathbb{V}(\mathfrak{a})\big)$$

(ii) If R is an infinite integral domain and $X \subseteq R^I$ is an algebraic set, then the vanishing ideal of the pull-back of X is just the pushed-out vanishing ideal of X, that is

$$\mathbb{I}\Big(\big(\pi_I^J\big)^{-1}(X)\Big) \;\;=\;\; \mathbb{I}(X)\,R[J]$$

(iii) In particular: If R is an algebraically closed field with $|I| < |R|$ and $\mathfrak{u} \trianglelefteq_{\mathfrak{i}} R[J]$ is an ideal of the form $\mathfrak{u} = \mathfrak{a}\,R[J]$ for some $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R[I]$, then we get

$$\mathbb{I}\,\mathbb{V}(\mathfrak{u}) \;\;=\;\; \sqrt{\mathfrak{u}}$$

Proof of (8.58):

(i) The unit element of $A/\mathfrak{a}$ is $1_A + \mathfrak{a}$, the R-algebra homomorphism is required to map $\varphi(1_A + \mathfrak{a}) = 1_R$. Thus for any $a \in R$ we get $\varphi(a1_A + \mathfrak{a}) = a\varphi(1_A + \mathfrak{a}) = a1_R = a$, as $a1_A + \mathfrak{a} = a(1_A + \mathfrak{a})$ and φ is R-linear. In particular $\mathrm{im}(\varphi) = R$. Suppose $\varphi = 0$, then we had $\varphi(1_A + \mathfrak{a}) = 0_R$ which would mean $0_R = 1_R$, in contradiction to $R \neq 0$.

(ii) In a first step, let us prove, that R is a field: So consider any $a \in R$ with $a \notin R^*$, we need to prove $a = 0$. To see this define the ideals $\mathfrak{h} := \langle t_i \mid i \in I\rangle$ and $\mathfrak{a} := \mathfrak{h} + aA$. That is $\mathfrak{a}$ is generated by $a1_A \in A$ and all the variables $t_i \in A$. Now regard the homomorphism

$$A \;\twoheadrightarrow\; R\Big/_{aR} \;:\; f \;\mapsto\; f[0] + aR$$

Clearly $\mathfrak{a}$ is contained in the kernel of this homomorphism. Conversely, if $f[0] + aR = 0 + aR$, then $f[0] = ab$ for some $b \in R$. Hence $f - ab \in \mathfrak{h}$ and from this we get $f \in \mathfrak{h} + ab \subseteq \mathfrak{a}$. Thus $\mathfrak{a}$ is the kernel of the above homomorphism and therefore $A/\mathfrak{a}$ and R/aR are isomorphic as R-algebras. If we had $\mathfrak{a} = A$ then R/aR would have to be zero, such that $aR = R$ in contradiction, to $a \notin R^*$. We conclude that $\mathfrak{a}$ is a proper ideal. Hence, by assumption there is a homomorphism φ of the form $\varphi : A/\mathfrak{a} \to R$ and by (i) we know that this is surjective

$$R\Big/_{aR} \;\xrightarrow{\sim}\; A\Big/_{\mathfrak{a}} \;\twoheadrightarrow\; R$$

In particular $R/aR \twoheadrightarrow R : b + aR \mapsto b1_A + \mathfrak{a} \mapsto \varphi(b1_A + \mathfrak{a}) = b$ is surjective. But as $a + aR \mapsto a$ and $a + aR = 0 + aR \mapsto 0$ the well-definedness of this map yields $a = 0$.

(ii) We have just proved, that R is a field, it remains to show, that R even is algebraically closed: To do this fix any $j \in I$, let $H := I \setminus \{j\}$ and consider an arbitrary, non-constant polynomial $f \in R[t_j] \subseteq A$ over R. Now define the ideals $\mathfrak{h} := \langle t_i \mid i \in H \rangle$ and $\mathfrak{a} := fA + \mathfrak{h}$. That is $\mathfrak{a}$ is generated by f and all the t_i with $i \neq j$. Then it is clear, that $R[t_j] \xrightarrow{\sim} A/\mathfrak{h} : g \mapsto g + \mathfrak{h}$ is an isomorphism of R-algebras, that maps $fR[t_j]$ to $\mathfrak{a}/\mathfrak{h}$. And therefore we find an isomorphism of the form

$$R[t_j] \Big/ fR[t_j] \xrightarrow{\sim} A/\mathfrak{h} \Big/ \mathfrak{a}/\mathfrak{h} \xrightarrow{\sim} A \Big/ \mathfrak{a} : g + fR[t_j] \mapsto g + \mathfrak{a}$$

Now $R[t_j]/fR[t_j]$ is a $\deg(f)$-dimensional R-vector space and as f is non-constant, we have $\deg(f) \geq 1$. In particular $R[t_j]/fR[t_j] \neq 0$ and therefore $A/\mathfrak{a} \neq 0$. That is $\mathfrak{a}$ is a proper ideal and by assumption there is a homomorphism φ of R-algebras such that we can build up the chain

$$\varphi : R[t_j] \Big/ fR[t_j] \xrightarrow{\sim} A \Big/ \mathfrak{a} \twoheadrightarrow R$$

Abbreviate the ideal $\mathfrak{f} := fR[t_j]$ and let $x := \varphi(t_j + \mathfrak{f}) \in R$. As φ is a homomorphism of R-algebras, it commutes with polynomials and hence we can compute

$$f(x) = f\big(\varphi(t_j + \mathfrak{f})\big) = \varphi\big(f(t_j + \mathfrak{f})\big) = \varphi\big(f(t_j) + \mathfrak{f}\big) = \varphi(f + \mathfrak{f}) = 0_R$$

as $f \in \mathfrak{f}$. Thus we have found a root $x \in R$ of f. As f was an arbitrary non-constant polynomial, this means *any* non-constant polynomial over R has a root, which means R is algebraically closed.

(iii) Let us first verify $\mathbb{V}(\mathfrak{m}_x) = \{x\}$: If $y \in \mathbb{V}(\mathfrak{m}_x)$, then for any $i \in I$ we can compute $0 = (t_i - x_i)(y_i) = y_i - x_i$ and hence $y_i = x_i$. That is $y = x$, so we have the inclusion from left to right. Conversely if $f \in \mathfrak{m}_x$, then there is a finite subset $\Omega \subseteq I$ such that

$$f(t) = \sum_{i \in \Omega} f_i(t) \cdot (t_i - x_i)$$

for some $f_i \in A$. But then we get $f(x) = \sum_i f_i(x)(x_i - x_i) = 0$ and as this is true for any $f \in \mathfrak{m}_x$ we found $x \in \mathbb{V}(\mathfrak{m}_x)$, which is the inclusion from right to left.

(iii) To continue we need a short preparation: For any $x = (x_i) \in R^I$ let us define the R-algebra homomorphism α_x by algebraic expansion of $t_i \mapsto t_i - x_i$ that is

$$\alpha_x : A \to A : f(t) \mapsto f(t - x)$$

These homomorphisms clearly satisfy $\alpha_x \alpha_{-x} = \mathbb{1}_A$ and $\alpha_{-x} \alpha_x = \mathbb{1}_A$ such that they are automorphisms. And by construction it also is clear, that

$$\alpha_x(\mathfrak{m}_0) = \mathfrak{m}_x$$

Let us first consider $x = 0$, then for any $f \in A$ we get $\varepsilon_0(f) = f(0) = f[0]$ such that $\varepsilon_0(f) = 0$ is

equivalent to $f \in \mathfrak{m}_0$. That is we have

$$\mathsf{kn}\big(\varepsilon_0\big) \;=\; \mathfrak{m}_0$$

Now for any $f \in A$ and any $x \in R^I$ compute $\varepsilon_x \alpha_x(f) = \alpha_x(f)(x) = f(x-x) = f(0)$. That is $\alpha_x(f) \in \mathsf{kn}(\varepsilon_x)$ is equivalent to $f(0) = 0$ which in turn is equivalent to $f \in \mathfrak{m}_0$. If we apply α_x to $f \in \mathfrak{m}_0 = \alpha_{-x}(\mathfrak{m}_x)$ we see that $f \in \mathfrak{m}_0$ equivalent to $\alpha_x(f) \in \mathfrak{m}_x$. Thus for $g := \alpha_x(f)$ we have $g \in \mathsf{kn}(\varepsilon_x)$ if and only if $g \in \mathfrak{m}_x$. And as α_x is surjective (even bijective) this is

$$\mathsf{kn}\big(\varepsilon_x\big) \;=\; \mathfrak{m}_x$$

Let us take a look at $\mathbb{I}(x) = \{\, f \in A \mid f(x) = 0 \,\}$. We see, that this is precisely the definition of $\mathsf{kn}(\varepsilon_x)$, such that the above identity can be extended, to

$$\mathbb{I}(x) \;=\; \mathsf{kn}\big(\varepsilon_x\big) \;=\; \mathfrak{m}_x$$

(iv) Consider any $g \in \sqrt{\mathfrak{a}}$, that is $g^n \in \mathfrak{a}$ for some $n \in \mathbb{N}$, then we need to show $g \in \mathbb{IV}(\mathfrak{a})$. More explicitly we need to verify $g(x) = 0$ for any $x \in \mathbb{V}(\mathfrak{a})$. As $x \in \mathbb{V}(\mathfrak{a})$ we have $f(x) = 0$ for any $f \in \mathfrak{a}$, in particular $g^n(x) = 0$. But this is $g(x)^n = 0$ and as R is reduced this implies $g(x) = 0$. As this is true for any $x \in \mathbb{V}(\mathfrak{a})$, we are done.

□

Proof of (8.59):

(i) Let us first prove, that any ideal of the form $\mathfrak{m}_x$ is maximal: For $x = 0 \in F^I$ we have $\mathfrak{m}_0 = \langle t_i \mid i \in I \rangle$ and thereby a canonical isomorphism of the form

$$F \;\xrightarrow{\sim}\; A\Big/_{\mathfrak{m}_0} \,:\, a \mapsto a1_A + \mathfrak{m}_0$$

And as F is a field, this means $A/\mathfrak{m}_0$ is, as well, such that $\mathfrak{m}_0$ is a maximal ideal of A. But as $\mathfrak{m}_x = \alpha_x(\mathfrak{m}_0)$ and α_x is an automorphism of A by (refer to the proof of 8.58.(iii)) and $\mathfrak{m}_0$ is a maximal ideal, so are all the ideals $\mathfrak{m}_x$.

The injectivity of the map $x \mapsto \mathfrak{m}_x$ is easy to see: Consider any two points $x = (x_i)$ and $y = (y_i) \in F^I$ such that $\mathfrak{m}_x = \mathfrak{m}_y$. Then for any $i \in I$ we have $t_i - x_i \in \mathfrak{m}_y$. In particular $x_i - y_i = (t_i - y_i) - (t_i - x_i) \in \mathfrak{m}_y$. If we had $x_i \neq y_i$ then $x_i - y_i \in F^* = A^*$ is a unit and hence $\mathfrak{m}_y = A$ in contradiction to the maximality of $\mathfrak{m}_y$. Thus we have $x_i = y_i$ for any $i \in I$ and hence $x = y$.

(ii) Let us first prove the correspondence for the maximal spectrum of $A/\mathfrak{a}$: If $\overline{\mathfrak{m}} \trianglelefteq_{\mathrm{i}} A/\mathfrak{a}$ is a maximal ideal, then by the correspondence theorem of ideals it is of the form $\overline{\mathfrak{m}} = \mathfrak{m}/\mathfrak{a}$ for some $\mathfrak{m} \in \mathsf{Smax}(A)$ with $\mathfrak{a} \subseteq \mathfrak{m}$. By assumption this means $\mathfrak{m} = \mathfrak{m}_x$ for some $x \in F^I$. As $\mathfrak{a} \subseteq \mathfrak{m} = \mathfrak{m}_x$ we get $\mathbb{V}(\mathfrak{m}_x) \subseteq \mathbb{V}(\mathfrak{a})$, but $\mathbb{V}(\mathfrak{m}_x) = \{\, x \,\}$ is clear, such that we have $x \in \mathbb{V}(\mathfrak{a})$. Altogether we have

$$\mathsf{Smax}\left(A\Big/_{\mathfrak{a}}\right) \;\subseteq\; \left\{ \mathfrak{m}_x\Big/_{\mathfrak{a}} \;\middle|\; x \in \mathbb{V}(\mathfrak{a}) \right\}$$

Conversely consider any $x \in \mathbb{V}(\mathfrak{a})$, then $\mathfrak{m}_x \trianglelefteq_{\mathrm{i}} A$ is maximal by (i). Applying $\mathbb{I}$ we get $\mathfrak{a} \subseteq \mathbb{IV}(\mathfrak{a}) \subseteq \mathbb{I}(x)$. But $\mathbb{I}(x) = \mathsf{kn}(\varepsilon_x) = \mathfrak{m}_x$ by (8.58.(iii)) such that we have $\mathfrak{a} \subseteq \mathfrak{m}_x$ and hence

$\mathfrak{m}_x/\mathfrak{a} \trianglelefteq_{\mathrm{i}} A/\mathfrak{a}$ is maximal, by the correspondence theorem of ideals.

That is the map $x \mapsto \mathfrak{m}_x/\mathfrak{a}$ is well-defined and surjective. It remains to prove its injectivity: If $\mathfrak{m}_x/\mathfrak{a} = \mathfrak{m}_x/\mathfrak{a}$, then $\mathfrak{m}_x = \mathfrak{m}_y$ because of the correspondence of ideals, but from this we already get $x = y$, according to (i).

(ii) Now for the second part: The correspondence of the maximal spectrum and the homomorphisms of F-algebras: If we start with a maximal ideal $\mathfrak{m}_x/\mathfrak{a}$ (that is $x \in \mathbb{V}(\mathfrak{a})$), then we have to show that ε_x is well defined. So consider any two $f, g \in A$ with $f + \mathfrak{a} = g + \mathfrak{a}$. That is $d := f - g \in \mathfrak{a} \subseteq \mathbb{IV}(\mathfrak{a})$. As $x \in \mathbb{V}(\mathfrak{a})$ and $d \in \mathbb{IV}(\mathfrak{a})$ we have $d(x) = 0$, which is $f(x) = g(x)$. Thus ε_x is well-defined.

If we start with $\varphi : A/\mathfrak{a} \to F$, then φ is surjective by (i) and hence $(A/\mathfrak{a})/\mathrm{kn}(\varphi)$ is isomorphic to F, which is a field and hence $\mathrm{kn}(\varphi) \trianglelefteq_{\mathrm{i}} A/\mathfrak{a}$ is a maximal ideal. Thus the converse map is well-defined, too. It remains to prove, that they are mutally inverse:

If we start with a maximal ideal $\overline{\mathfrak{m}} = \mathfrak{m}_x/\mathfrak{a}$ of $A/\mathfrak{a}$ we have to verify that $\mathrm{kn}(\varepsilon_x)$ is $\mathfrak{m}_x/\mathfrak{a}$ again: But as we have seen in (8.58.(iii)) $\mathrm{kn}(\varepsilon_x) = \{ f + \mathfrak{a} \mid f(x) = 0 \} = \mathfrak{m}_x/\mathfrak{a}$ is satisfied. Conversely, if we start with a homomorphism φ, then $\mathrm{kn}(\varphi) = \mathfrak{m}_x/\mathfrak{a}$ for some $x \in \mathbb{V}(\mathfrak{a})$. So we have to verify $\varphi = \varepsilon_x$: That is we consider any $f \in A$ and have to show $\varphi(f + \mathfrak{a}) = \varepsilon_x(f + \mathfrak{a}) = f(x)$.

Let $a := \varphi(f + \mathfrak{a})$, then by (8.58.(i)) we have $\varphi(a1_A + \mathfrak{a}) = a = \varphi(f + \mathfrak{a})$ and therefore $(f - a1_A) + \mathfrak{a} \in \mathrm{kn}(\varphi) = \mathfrak{m}_x/\mathfrak{a}$. Thus we found $f - a1_A \in \mathfrak{m}_x$, which is nothing but $f(x) = a1_A(x) = a$. Therefore $\varepsilon_x(f + \mathfrak{a}) = f(x) = a = \varphi(f + \mathfrak{a})$ such that $\varphi = \varepsilon_x$.

- Nota Item (iii) is the classical Hilbert's Nullstellensatz. As this is a most famous result, we will give 2 alternative proofs: The first is due to O. Zariski who saw an application of Noetherian normalization here. The second is an application of Jacobson rings and it's merit is due to several mathematicians, primarily W. Krull, and O. Goldman.

(iii) *Zariski's Proof:* As I is non-empty and finite, we may assume $I = \{ 1, \ldots, n \}$ for some $1 \leq n \in \mathbb{N}$. Consider any maximal ideal $\mathfrak{m} \trianglelefteq_{\mathrm{i}} A$ and let $L := A/\mathfrak{m}$. Then L is a finitely generated F-algebra, as $L = F[t_1 + \mathfrak{m}, \ldots, t_n + \mathfrak{m}]$. By the Noetherian normalization theorem, there is an algebraically independent set $\{ z_1, \ldots, z_r \} \subseteq L$ such that for $K := F[z_1, \ldots, z_r]$ the extension $L : K$ is finite (we also know $r \leq n$, but this is irrelevant here). In particular $L : K$ is an integral extension of rings.

As $\mathfrak{m}$ is a maximal ideal L is a field and as $K \subseteq L$, L also is torsion-free, as a K-module. As $L : K$ is integral, this implies K to be a field, too. Suppose $r \geq 1$, then $z_1^{-1} \in K$, that is $z_1 f(z_1, \ldots, z_r) = 1_L$ for some $f \in F[t_1, \ldots, t_r]$. But then $0 = \deg_1(1_L) = 1 + \deg_1(f)$, which is absurd. Hence we find $r = 0$, that is $K = F1_L$. That is $L : F$ is finite, say $m := [L : F]$. Hence any $x \in L$ satisfies an equation $g \in F[t]$ of degree $\deg(g) \leq m + 1$. But F was assumed to be algebraically closed hence $g(x) = 0$ implies $x \in F\,1_L$ and therefore

$$\alpha : F \xrightarrow{\sim} L : a \mapsto a1_L$$

is surjective. And as F is a field and $\alpha \neq 0$ it also is injective. Pick up $x_i \in F$ such that $x_i + \mathfrak{m} = x_i 1_L = t_i + \mathfrak{m} \in A/\mathfrak{m} = L$. Then for any $i \in 1 \ldots n$ we get $t_i - x_i \in \mathfrak{m}$ and hence $\mathfrak{m}_x \subseteq \mathfrak{m}$. As F is a field, $\mathfrak{m}_x$ is maximal and $\mathfrak{m} \neq A$ such that $\mathfrak{m}_x = \mathfrak{m}$.

(iii) *Goldman-Like Proof:* As I is non-empty and finite, we may assume $I = 1 \dots n$ for some $1 \leq n \in \mathbb{N}$. Then we use induction on n, starting with $n = 1$, that is $A = F[s]$ for $s := t_1$. Consider any maximal ideal $\mathfrak{m} \trianglelefteq_{\mathrm{i}} F[s]$, then $\mathfrak{m} = gF[s]$ for some $g \in F[s]$. As $\mathfrak{m} \neq F[s]$ we have $g \notin F[s]^* = F^*$, that is g is non-constant. As F is algebraically closed, this means $g(x) = 0$ for some $x \in F$ and thereby $s - x \mid g$. By maximality of $\mathfrak{m} = gF[s] \subseteq \langle s - x \rangle = \mathfrak{m}_x$ we have $\mathfrak{m} = \mathfrak{m}_x$ which means that $F[s]$ is geometric.

Now for the induction step: We already know that $A = F[t_1, \dots, t_n]$ is geometric and have to prove that $F[t_1, \dots, t_n, t_{n+1}] = A[s]$ for $s := t_{n+1}$ is geometric, too. Thus we consider any maximal ideal $\mathfrak{n} \trianglelefteq_{\mathrm{i}} A[s]$. As F is a field, it also is a Jacobson ring and hence A and $A[s]$ are Jacobson rings, too, according to (2.170.(iv)). One of the equivalent properties of A being jacobson is that $\mathfrak{m} := \mathfrak{n} \cap A$ is a maximal ideal again, as we have seen in (2.171.(iii)). By induction hypothesis there then is some $x \in F^n$ such that $\mathfrak{m} = \mathfrak{m}_x$. Now consider the epimorphism

$$\varepsilon_x \ : \ A[s] \ \twoheadrightarrow \ F[s] \ : \ g(t)(s) \mapsto g(x)(s)$$

Consider $g \in A[s]$ in the form $g(t)(s) = \sum_k g_k(t)s^k$ for some $g_k \in A$. Then we get $\varepsilon_x(g) = g(x)(s) = \sum_k g_k(x)s^k = 0$ if and only $g_k(x) = 0$ for any $k \in \mathbb{N}$. This again is $g_k \in \mathfrak{m}_x$ (for any $k \in \mathbb{N}$) and thereby we get

$$\mathsf{kn}\big(\varepsilon_x\big) \ = \ \mathfrak{m}_x[s]$$

As ε_x is surjective we find that this induces an isomorphism of F-algebras, of the form

$$\bar{\varepsilon}_x \ : \ A[s] \Big/ \mathfrak{m}_x[s] \ \xrightarrow{\sim} \ F[s] \ : \ g(t)(s) + \mathfrak{m}_x[s] \mapsto g(x)(s)$$

As $\mathfrak{n}$ is maximal and $\mathfrak{m}_x[s] = (\mathfrak{n} \cap A)[s] \subseteq \mathfrak{n}$ we find that $\mathfrak{n}/\mathfrak{m}_x$ is a maximal ideal of $A/\mathfrak{m}_x[s]$. This is transferred to $F[s]$ under $\bar{\varepsilon}_x$, that is we have

$$\bar{\varepsilon}_x \left(\mathfrak{n} \Big/ \mathfrak{m}_x[s] \right) \ \in \ \mathsf{Smax}\big(F[s]\big)$$

By the case $n = 1$ this means that this ideal is of the form $(s - y)F[s]$ for some $y \in F$. In other words $t_{n+1} - y + \mathfrak{m}_x[s] \in \mathfrak{n}/\mathfrak{m}_x[s]$, which is $t_{n+1} - y \in \mathfrak{n}$. But as for any $k \in 1 \dots n$ we also have $t_k - x_k \in \mathfrak{m}_x = \mathfrak{n} \cap A$ we find $\mathfrak{m}_{(x,y)} \subseteq \mathfrak{n}$. And by the maximality of $\mathfrak{m}_{(x,y)}$ this implies $\mathfrak{m}_{(x,y)} = \mathfrak{n}$, that is $A[s]$ is geometric again.

(iv) Let us now consider an infinite set I, that is there is a subset $\Omega := \{\, i(n) \mid n \in \mathbb{N} \,\} \subseteq I$. Then we can use this subset to shift the variables t_i of A according to $t_{i(n)} \mapsto t_{i(n-1)}$ for $1 \leq n \in \mathbb{N}$ and $t_i \mapsto t_i$ for $i \notin \Omega$. Then we freed up $t_{i(0)} \mapsto s$ and thereby gain an isomorphism of F-algebras, by extension of

$$\Phi \ : \ A \ \xrightarrow{\sim} \ A[s] \ : \ t_i \mapsto \begin{cases} s \text{ if } i = i(0) \\ t_{i(n)} \text{ if } i = i(n+1) \\ t_i \text{ if } i \notin \Omega \end{cases}$$

If now $x = (x_i) \in F^I$, then we need to shift $x \mapsto x' := (x'_i)$ where $x'_{i(n)} := x_{i(n+1)}$ for $n \in \mathbb{N}$,

$x'_i := x_i$ for $i \notin \Omega$ and $y := x_{i(0)}$. Then it is clear that this isomorphism links the maximal ideals

$$\Phi(\mathfrak{m}_x) \;=\; \mathfrak{m}_{(x',y)}$$

Thus, if A is geometric and $\mathfrak{n} \trianglelefteq_{\mathrm{i}} A[s]$ is a maximal ideal, then $\Phi^{-1}(\mathfrak{m}) \trianglelefteq_{\mathrm{i}} A$ is a maximal ideal, as well. Hence we find an $x \in F^I$ such that $\Phi(\mathfrak{n}) = \mathfrak{m}_x$ and therefore $\mathfrak{n} = \Phi(\mathfrak{m}_x) = \mathfrak{m}_{(x',y)} \trianglelefteq_{\mathrm{i}} A[s]$. As we can do this for any maximal ideal $\mathfrak{n}$ of $A[s]$ we see that $A[s]$ is geometric again. The converse direction is just the same thing, using the transfer of $\mathfrak{m} \trianglelefteq_{\mathrm{i}} A$ to $A[s]$ under Φ^{-1}.

□

Proof of (8.60):
We will first prove the equivalence of the statements (b) to (h) in pairs. Note that due to (8.58.(ii)) property (b) implies that F is an algebraically closed field. Thus whenever we have (b) on our side, we may assume F to be a field (an even algebraically closed one).

- The implication (b) $\implies$ (c) is trivial, we have to commit ourselves to (c) $\implies$ (b) only: For this we simply choose a maximal ideal $\mathfrak{m} \trianglelefteq_{\mathrm{i}} A$, such that $\mathfrak{a} \subseteq \mathfrak{m}$. Then we obtain a well-defined homomorphism
$$\varrho \;:\; {}^{A}\!\Big/_{\mathfrak{a}} \twoheadrightarrow {}^{A}\!\Big/_{\mathfrak{m}} \;:\; f + \mathfrak{a} \mapsto f + \mathfrak{m}$$
and by assumption (c) there also is a homomorphism $\varphi : A/\mathfrak{m} \to F$. Thus by composition $\varphi\varrho$ we get the desired homomorphism from $A/\mathfrak{a}$ to F.

- The next step will be (d) $\implies$ (c): Consider any maximal ideal $\mathfrak{m} \trianglelefteq_{\mathrm{i}} A$, then we have to find a homomorphism φ of R-algebras, of the form $\varphi : A/\mathfrak{m} \to F$. By assumption (d) there is some $x \in F^I$ such that $\mathfrak{m} = \mathfrak{m}_x$, thus the candidate is $\varepsilon_x : A \to F : f \mapsto f(x)$. By (8.58.(iii)) we have $\mathrm{kn}(\varepsilon_x) = \mathfrak{m}_x = \mathfrak{m}$ and thereby ε_x induces φ via
$$\varphi \;:\; {}^{A}\!\Big/_{\mathfrak{m}} \to F \;:\; f + \mathfrak{m} \mapsto f(x)$$
For the converse direction (c) $\implies$ (d) we are given any maximal ideal $\mathfrak{m} \trianglelefteq_{\mathrm{i}} A$ and have to find some $x \in F^I$ such that $\mathfrak{m} = \mathfrak{m}_x$. With (c) comes (b) and hence F is a field here. And by assumption (c) there is a homomorphism φ of the form $\varphi : A/\mathfrak{m} \to F$. By (8.58.(i)) φ is surjective and $\varphi \neq 0$. Now consider $\mathrm{kn}(\varphi) \trianglelefteq_{\mathrm{i}} A/\mathfrak{m}$. As $\mathfrak{m}$ is maximal, $A/\mathfrak{m}$ is a field, such that either $\mathrm{kn}(\varphi) = 0$ or $\mathrm{kn}(\varphi) = A/\mathfrak{m}$. The latter is ruled out, by $\varphi \neq 0$ and hence φ also is injective. Altogether we have an isomorphism
$$\varphi \;:\; {}^{A}\!\Big/_{\mathfrak{m}} \xrightarrow{\sim} F$$
of F-algebras. For any $i \in I$ let $x_i := \varphi(t_i + \mathfrak{m}) \in F$ and $x := (x_i)$, then we have $\varphi(t_i - x_i 1_A + \mathfrak{m}) = \varphi(t_i + \mathfrak{m}) - x_i\varphi(1_A + \mathfrak{m}) = x_i - x_i = 0$. Thus $t_i - x_i 1_A + \mathfrak{m} \in \mathrm{kn}(\varphi) = 0$ such that $t_i - x_i 1_A \in \mathfrak{m}$. As this is true for any $i \in I$ we get $\mathfrak{m}_x \subseteq \mathfrak{m}$. But as F is a field, $\mathfrak{m}_x$ is a maximal ideal, by (8.58.(v)) and as $\mathfrak{m} \neq A$ this implies $\mathfrak{m}_x = \mathfrak{m}$.

- The implication (e) $\implies$ (d) is trivial again, it is the surjectivity of the correspondence in (e). For the converse direction (d) $\implies$ (e), we also got (b) from (d) and hence F is a field. Therefore (8.59.(i)) already tells us, that the map $x \mapsto \mathfrak{m}_x$ is well-defined and injective. And if $\mathfrak{m} \trianglelefteq_{\mathrm{i}} A$ is

any maximal ideal, then by assumption (d) there is some $x \in F^I$ such that $\mathfrak{m} = \mathfrak{m}_x$. This also is the surjectivity of $x \mapsto \mathfrak{m}_x$ and hence the correspondence.

- Property (f) is just a reformulation of (d), of finite kind. Let us deal with the case $\Omega = \emptyset$ first: In this case $F[t_i \mid i \in \Omega] = F$ and $\langle t_i - a_i \mid i \in \Omega \rangle = \langle \emptyset \rangle = 0$. Thus (f) reads as $\mathfrak{m} \cap F = 0$ for any $\mathfrak{m} \in \operatorname{Smax}(A)$. If F is a field, then $\mathfrak{m} \cap F = 0$ is clear, as 0 is the only proper ideal of F and $\mathfrak{m} \cap F$ even is a prime ideal of F. Conversely, we assume $A \cap \mathfrak{m} = 0$ for any $\mathfrak{m} \in \operatorname{Smax}(A)$ and need to show that F is a field: Consider any $a \in F \setminus F^*$. Then $aF \trianglelefteq_{\mathfrak{i}} F$ is a proper ideal and hence there is a maximal ideal $\mathfrak{m}_0 \in \operatorname{Smax}(F)$ containing $aF \subseteq \mathfrak{m}_0$. Then $\mathfrak{m} := \{ f \in A \mid f(0) \in \mathfrak{m}_0 \}$ is a maximal ideal of A. Yet $a \in \mathfrak{m}_0 = \mathfrak{m} \cap F = 0$ implies $a = 0$ and as a has been arbitrary we conclude $F \setminus \{0\} = F^*$, which means F is a field.

 We start by proving (d) $\implies$ (f): With (d) comes (b) and hence we find that F is a field. Now, if $\Omega \subseteq I$ is a non-empty finite set and $\mathfrak{m} \trianglelefteq_{\mathfrak{i}} A$ is a maximal ideal, then by assumption (d) we have $\mathfrak{m} = \mathfrak{m}_x$. That is for any $i \in I$ there is some $x_i \in F$, such that $t_i - x_i \in \mathfrak{m}_x = \mathfrak{m}$. For $i \in \Omega$ we also have $t_i - x_i \in A_0 := F[t_i \mid i \in \Omega]$ and therefore

 $$\langle t_i - x_i \mid i \in \Omega \rangle \quad \subseteq \quad \mathfrak{m} \cap A_0$$

 As F is a field $\langle t_i - x_i \mid i \in \Omega \rangle$ is a maximal ideal of A_0, according to (8.59.(i)). Yet $\mathfrak{m} \cap A_0$ is a proper ideal (even a prime ideal) and therefore this inclusion turns into an identity again.

 Conversely for (f) $\implies$ (d) we find that F is a field, by taking $\Omega = \emptyset$. We now start with a maximal ideal $\mathfrak{m}$ and have to find some $x \in F^I$, such that $\mathfrak{m} = \mathfrak{m}_x$. To do this pick up an arbitrary $i \in I$. Then $\Omega := \{i\} \subseteq I$ is a finite set and hence by assumption (f) we have $\mathfrak{m} \cap F[t_i] = \langle t_i - x_i \rangle$ for some $x_i \in F$. As we can do this with any $i \in I$ we find a point $x = (x_i) \in F^I$ with $t_i - x_i \in \mathfrak{m}$ for any $i \in I$. That is $\mathfrak{m}_x \subseteq \mathfrak{m}$. As F is a field $\mathfrak{m}_x$ is a maximal ideal of A, by (8.59.(i)) again. And as $\mathfrak{m}$ is proper (even maximal) the inclusion $\mathfrak{m}_x \subseteq \mathfrak{m}$ turns into the identity desired $\mathfrak{m}_x = \mathfrak{m}$.

- The step (d) $\implies$ (g) is easy again: With (d) we also have (b) and hence F is a field. And if $\mathfrak{a} = A$, then $1_A \in \mathfrak{a}$ and hence $\mathbb{V}(\mathfrak{a}) \subseteq \mathbb{V}(1_A) = \emptyset$. Conversely, if $\mathfrak{a} \neq A$, then there is a maximal ideal $\mathfrak{m} \trianglelefteq_{\mathfrak{i}} A$ such that $\mathfrak{a} \subseteq \mathfrak{m}$. And by assumption (d) we have $\mathfrak{m} = \mathfrak{m}_x$ for some $x \in F^I$. Thereby $\{ x \} = \mathbb{V}(\mathfrak{m}_x) = \mathbb{V}(\mathfrak{m}) \subseteq \mathbb{V}(\mathfrak{a})$ and in particular $\mathbb{V}(\mathfrak{a}) \neq \emptyset$ is non-empty.

 Conversely for (g) $\implies$ (d) we are given some maximal ideal $\mathfrak{m} \trianglelefteq_{\mathfrak{i}} A$. As $\mathfrak{m} \neq A$ we have $\mathbb{V}(\mathfrak{m}) \neq \emptyset$ by assumption (g). Thus there is some $x \in F^I$ with $x \in \mathbb{V}(\mathfrak{m})$. That is for any $f \in \mathfrak{m}$ we have $f(x) = 0$, which can be put as $f \in \operatorname{kn}(\varepsilon_x)$. In other words we find the inclusion $\mathfrak{m} \subseteq \operatorname{kn}(\varepsilon_x) = \mathfrak{m}_x$ by (8.58.(iii)). But from this, as $\mathfrak{m}$ is maximal and $\mathfrak{m}_x \neq A$, we conclude $\mathfrak{m} = \mathfrak{m}_x$.

- Let us get to the bottom of this (g) $\implies$ (h): With (g) we have (b) and hence know, that F is a field (even algebraically closed). Now define the evaluation homomorphism

 $$\varepsilon \; : \; A \; \twoheadrightarrow \; F[U] \; : \; t_i \mapsto u_i$$

 As this is surjective, we have $A/\operatorname{kn}(\varepsilon) \xrightarrow{\sim} F[U]$ under $f + \operatorname{kn}(\varepsilon) \mapsto \varepsilon(f) = f(u)$. As $F[U]$ is assumed to be a field, $\operatorname{kn}(\varepsilon)$ is a maximal ideal of A. Thus by assumption there is some $x \in F^I$

with $x \in \mathbb{V}(\ker(\varepsilon))$. Then we find

$$\ker(\varepsilon) \quad \subseteq \quad \mathbb{IV}\big(\ker(\varepsilon)\big) \quad \subseteq \quad \mathbb{I}(x) \quad = \quad \mathfrak{m}_x$$

But $\ker(\varepsilon)$ is maximal and $\mathfrak{m}_x$ is proper, such that we have $\ker(\varepsilon) = \mathfrak{m}_x$. Now consider the following isomorphisms, as these can be composed to yield the desired isomorphism

$$\begin{array}{ccccccc} F[U] & \xrightarrow{\sim} & A\big/_{\ker(\varepsilon)} & = & A\big/_{\mathfrak{m}_x} & \xrightarrow{\sim} & F \\ \varepsilon(f) & \mapsto & f + \ker(\varepsilon) & = & f + \mathfrak{m}_x & \mapsto & f(x) \end{array}$$

Let us proceed with (h) $\implies$ (g): If $\mathfrak{a} = A$, then $1_A \in \mathfrak{a}$ and hence $\mathbb{V}(\mathfrak{a}) \subseteq \mathbb{V}(1_A) = \emptyset$. Conversely consider a proper ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} A$, then there is a maximal ideal $\mathfrak{m} \in \operatorname{Smax}(A)$ containing $\mathfrak{a} \subseteq \mathfrak{m}$. For any $i \in I$ let $u_i := t_i + \mathfrak{m}$, then $A/\mathfrak{m} = F[U]$. And as $\mathfrak{m}$ is maximal, this makes $F[U]$ a field. By assumption (h) there is an isomorphism

$$\Phi \;:\; A\big/_{\mathfrak{m}} \xrightarrow{\sim} F$$

Let $x_i := \Phi(u_i) \in F$ then we find $\Phi(t_i - x_i + \mathfrak{m}) = \Phi(t_i + \mathfrak{m}_i) - \Phi(x_i 1_A + \mathfrak{m}) = \Phi(u_i) - x_i\Phi(1_A + \mathfrak{m}) = x_i - x_i = 0_F$. As Φ is injective we conclude $t_i - x_i + \mathfrak{m} = 0 + \mathfrak{m}$ and thereby $t_i - x_i \in \mathfrak{m}$. As this is true for any $i \in I$, we have $\mathfrak{m}_x \subseteq \mathfrak{m}$. But F was assumed to be a field and hence $\mathfrak{m}_x$ is maximal, such that we get $\mathfrak{m}_x = \mathfrak{m}$. In particular $x \in \mathbb{V}(\mathfrak{m}_x) = \mathbb{V}(\mathfrak{m}) \subseteq \mathbb{V}(\mathfrak{a})$ such that $\mathbb{V}(\mathfrak{a}) \neq \emptyset$.

By now we have established the equivalencies of (b) to (h) and all of the proves have been more or less straightforward. Time to bring (i) into the fold, we will see that this already requires some more effort:

- The direction (i) $\implies$ (g) is clear: If $\mathfrak{a} = A$, then $1_A \in \mathfrak{a}$ and hence $\mathbb{V}(\mathfrak{a}) \subseteq \mathbb{V}(1_A) = \emptyset$. Conversely consider $\mathfrak{a} \trianglelefteq_{\mathrm{i}} A$ with $\mathbb{V}(\mathfrak{a}) = \emptyset$, then $\sqrt{\mathfrak{a}} = \mathbb{IV}(\mathfrak{a}) = \mathbb{I}(\emptyset) = A$ and thereby $1_A \in \sqrt{\mathfrak{a}}$. That is $1_A^n \in \mathfrak{a}$ for some $n \in \mathbb{N}$ which implies $1_A \in \mathfrak{a}$ and thereby $\mathfrak{a} = A$.

- So we finally set out for (d) $\implies$ (i), where we know that F is an algebraically closed field, as (d) implies (b). Note that the assumption (d) can be put as: A is geometric. If I is infinite, then by (8.59.(iv)) we know, that $A[s]$ is geometric, too. If I is finite, say $I = 1 \ldots n$, then $A[s] = A[s] = F[s, t_1, \ldots, t_n]$ is geometric in itself, because of (8.59.(iii)). So in both cases we get from (d), that $A[s]$ is geometric, too. That is $A[s]$ satisfies property (d) and we already know that this is equivalent to property (g). That is we have (g) for $A[s]$, as well.

 With this knowledge in mind, we can use *Rabinowitsch's trick*, which still works like charm, after all these years: As F is a reduced ring (even a field) we have $\sqrt{\mathfrak{a}} \subseteq \mathbb{IV}(\mathfrak{a})$ according to (8.58.(iv)). Thus we only need to check the converse inclusion, which is

$$\mathbb{IV}(\mathfrak{a}) \quad = \quad \{\, f \in A \mid \forall\, x \in \mathbb{V}(\mathfrak{a}) : f(x) = 0 \,\} \quad \subseteq \quad \sqrt{\mathfrak{a}}$$

 Note that the condition $\forall\, x \in \mathbb{V}(\mathfrak{a}) : f(x) = 0$ is equivalent to saying $\mathbb{V}(\mathfrak{a}) \subseteq \mathbb{V}(f)$. Now assume that f is such a polynomial. Then we introduce a new indeterminate s to the polynomial

ring $A = F[t_i \mid i \in I]$ and for any $a \in \mathfrak{a}$ we define the following polynomials in $A[s]$

$$\overline{a}(s,t) \;:=\; a(t) \quad \text{and} \quad b(s,t) \;:=\; 1 - s\,f(t)$$

We now claim that the algebraic set of all these polynomials is empty - that is

$$\mathbb{V}(\mathfrak{b}) \;=\; \emptyset \quad \text{where} \quad \mathfrak{b} \;:=\; \langle \{\, \overline{a} \mid a \in \mathfrak{a} \,\} \cup \{\, b \,\} \rangle \;\trianglelefteq_{\mathrm{i}}\; A[s]$$

In fact assume that $z = (x,y) \in F \times F^I$ was contained in $\mathbb{V}(\mathfrak{b})$. Then by construction all the $\overline{a}$ would vanish on z. As $0 = \overline{a}(z) = a(y)$ this would imply $y \in \mathbb{V}(\mathfrak{a}) \subseteq \mathbb{V}(f)$ such that

$$0 \;=\; b(z) \;=\; 1 - xf(y) \;=\; 1 - x \cdot 0 \;=\; 1$$

From this contradiction we get $\mathbb{V}(\mathfrak{b}) = \emptyset$ and since (we have for this argued above) $A[s]$ satisfies property (g) again, this means $\mathfrak{b} = A[s]$ and hence there are polynomials $g_1, \ldots, g_r, h \in A[s]$ and $a_1, \ldots, a_r \in \mathfrak{a}$ such that

$$1 \;=\; g_1\,a_1 + \cdots + g_r\,a_r + h \cdot (1 - s\,f)$$

We now map $A[s] \to \mathrm{QUOT}(A)$ by substituting $s \mapsto 1/f$. If the insert this equation into this map $1 - s\,f$ vanishes and we can multiply with a sufficiently high power $k \in \mathbb{N}$ to clear denominators to finally find

$$f^k \;=\; \widetilde{g}_1\,a_1 + \cdots + \widetilde{g}_r\,a_r$$

where $\widetilde{g}_i(t) = f^k(t) \cdot g_i(\frac{1}{f(t)}, t) \in A$ now are polynomials of A. In other words, f is contained in the radical of $\mathfrak{a}$, which had to be shown.

Altogether we have established the equivalencies of (b) to (i) and it remains to tackle (a). This is where the real work begins: The proof for (a) $\implies$ (d) is a generalization of the proof found in M. Brodmann, Algebraische Geometrie for $F = \mathbb{C}$ and the converse direction is due to S. Lang.

- We start with (a) $\implies$ (d): If I is finite, then $A = F[t_i \mid i \in I]$ is geometric, according to (8.59.(iii)) and this already is property (d). So we only have to consider the case, that I is infinite: By definition any polynomial $f \in A = F[t_i \mid i \in I]$ is an F-linear combination over the monomials t^α where $\alpha \in \mathbb{N}^{\oplus I}$. However, as I is infinite

$$|\mathbb{N}^{\oplus I}| \;=\; \max\{\, |\mathbb{N}|, |I| \,\} \;=\; |I|$$

We can choose any well-ordering on I and use the bijection $I \longleftrightarrow \mathbb{N}^{\oplus I} : i \mapsto \alpha_i$ to install a total order $\alpha_i \leq \alpha_j \;:\Longleftrightarrow\; i \leq j$. This need not be a monomial order, as this will not be required for the proof. Nevertheless, we may define the degree of a polynomial $f \in A$ in the obvious way

$$\deg(f) \;:=\; \max\Big\{\, \alpha \in \mathbb{N}^{\oplus I} \mid f[\alpha] \neq 0 \,\Big\}$$

If now $\beta \in \mathbb{N}^{\oplus I}$ is any multi-index then clearly $\{\, t^\alpha \mid \alpha \leq \beta \,\}$ corresponds to a subset of I. Hence the subspace of A generated by this set has dimension $|I|$, at most:

$$\Omega_\beta \;:=\; \{\, f \in A \mid \deg(f) \leq \beta \,\}$$

- Now consider some maximal ideal $\mathfrak{m} \trianglelefteq_{\mathrm{i}} A$. We need to show that $\mathfrak{m}$ belongs to some point $x = (x_i) \in F^I$. But by the maximality of $\mathfrak{m}_x$, it suffices to show $\mathfrak{m}_x \subseteq \mathfrak{m}$, which can be put as

$$\forall\, i \in I \;\; \exists\, x_i \in F \;\; : \;\; t_i - x_i \in \mathfrak{m}$$

Assume this was false, i.e. there was some $j \in I$ such that for any $z \in F$ we would get $t_j - z \notin \mathfrak{m}$. Formally the assumption for this j reads as

$$\forall\, z \in F \;\; : \;\; t_j - z \notin \mathfrak{m}$$

As $\mathfrak{m}$ is maximal this implies $\mathfrak{m} + (t_j - z)A = A$ and hence (for any $z \in F$) we may find polynomials $m^z \in \mathfrak{m}$ and $g^z \in A$ such that

$$\forall\, z \in F \;\; : \;\; m^z + (t_j - z)g^z \;=\; 1$$

Every polynomial g^z has a degree and hence F may be decomposed into a disjoint union of the following subsets

$$F \;\; = \;\; \bigsqcup_{i \in I} \{\, z \in F \mid \deg(g^z) = \alpha_i \,\}$$

If all these sets $F_i := \{\, z \in F \mid \deg(g^z) = \alpha_i \,\}$ would satisfy $|F_i| \leq |I|$ then there would be surjective maps $s_i : I \twoheadrightarrow F_i$ and thereby a surjective map $I \times I \twoheadrightarrow F : (h,i) \mapsto s_i(h)$. Yet as I is infinite we have $|I \times I| = |I| < |F|$ by assumption and (0.38.(iv)). Hence there cannot be a surjective map from $I \times I$ onto F. We conclude that there must be some $i \in I$ such that $|F_i| > |I|$. Let $\beta := \alpha_i$ and $Z := F_i$ for this $i \in I$, that is

$$Z \;\; := \;\; \{\, z \in F \mid \deg(g^z) = \beta \,\} \quad \text{satisfies} \quad |Z| \;>\; |I|$$

As we have seen Ω_β is an F-vectorspace of dimension at most $|I|$. If some of the g^z where $z \in Z$ were identical, then we could skip the next step and continue with the next linear relation, right away. If all the g^z where $z \in Z$ are distinct, then the set $\{\, g^z \mid z \in Z \,\}$ has cardinality $|Z| > |I| \geq \dim(\Omega_\beta)$. Thus the g^z have to satisfy a linear relation, that is there are pairwise distinct elements $z_1, \ldots, z_r \in Z$ and coefficients $\lambda_1, \ldots, \lambda_r \in F^*$ such that

$$\sum_{p=1}^{r} \lambda_p\, g^{z_p} \;\; = \;\; 0$$

We now define a specific polynomial $g \in F[t_j] \subseteq A$ in the one variable t_j over F

$$g \;\; := \;\; \sum_{p=1}^{r} \lambda_p \prod_{q \neq p} (t_j - z_q) \;\; \in \;\; F[t_j] \;\; \subseteq \;\; A$$

By construction we have $g(z_1) = \lambda_1 (z_1 - z_2) \ldots (z_1 - z_r) \neq 0$ and hence g is non-zero itself. We now claim that this polynomial is nevertheless contained in the ideal $\mathfrak{m}$

$$g \;\; = \;\; \sum_{p=1}^{r} \lambda_p \prod_{q \neq p} (t_j - z_q)$$

$$
\begin{aligned}
&= \sum_{p=1}^{r} \lambda_p [m^{z_p} + (t_j - z_p) g^{z_p}] \prod_{q \neq p} (t_j - z_q) \\
&= \sum_{p=1}^{r} \left[\lambda_p \prod_{q \neq p} (t_j - z_q) \right] m^{z_p} + \left[\sum_{p=1}^{r} \lambda_p \, g^{z_p} \right] \prod_{q=1}^{r} (t_j - z_q) \\
&= \sum_{p=1}^{r} \left[\lambda_p \prod_{q \neq p} (t_j - z_q) \right] m^{z_p} + 0 \quad \in \quad \mathfrak{m}
\end{aligned}
$$

That is, we have $g \in \mathfrak{m}$, if $g \in F$ was constant, then (as also $g \neq 0$) we had $g \in F^* = A^*$. But this cannot be, as $g \in \mathfrak{m}$ and $\mathfrak{m} \neq A$. In fact, as $\mathfrak{m}$ is maximal, it is a prime ideal and hence some prime factor of $g \in F[t_j]$ is contained in $\mathfrak{m}$. But as F is algebraically closed and $g \notin F$, the prime factors of g are of the form $t_j - z$ for some $z \in F$, in contradiction to $t_j - z \notin \mathfrak{m}$ for any $z \in F$.

- We turn our attention to (d) $\implies$ (a) now: We already know that (d) implies F to be algebraically closed, due to (8.58.(ii)) so it only remains to prove $|I| < |F|$. If I is finite, then $|I| < |F|$ is clear, as an algebraically closed field always is infinite. So from now on we assume, that I is infinite: Fix any $j \in I$, as I is infinite we have $|I \setminus \{j\}| = |I|$ and thereby there is a subset $H \subseteq I \setminus \{j\}$ such that $H \longleftrightarrow F : i \mapsto a_i$. We now define a homomorphism of F-algebras $\varphi : A \to F(s)$, by expansion of

$$
\begin{aligned}
\varphi(t_i) &:= 0 \quad \text{for} \quad i \in I \setminus \big(H \cup \{j\}\big) \\
\varphi(t_i) &:= s \quad \text{for} \quad i = j \\
\varphi(t_i) &:= \frac{1}{s - a_i} \quad \text{for} \quad i \in H
\end{aligned}
$$

We first have to check, that φ is surjective: As F is algebraically closed any polynomial $p(s) \in F[s]$ splits into linear factors, but as we have enumerated F using the index set H, we may write it in the form

$$
p(s) \quad = \quad \lambda \, (s - a)^{\alpha} \quad := \quad \lambda \prod_{i \in H} (s - a_i)^{\alpha_i}
$$

with only finitely many $\alpha_i \in \mathbb{N}$ being non-zero. Therefore any rational function p/q, where p, $q \in F[s]$ and $q \neq 0$, can be written in the following form, where $k_i \in \mathbb{Z}$ and only finitely many k_i are non-zero

$$
\frac{p(s)}{q(s)} \quad = \quad \lambda \prod_{i \in H} (s - a_i)^{k_i}
$$

By construction of φ it is clear, that any polynomial $f(t_j) \in F[t_j] \subseteq A$ is simply mapped to $f(s) \in F(s)$. Likewise any monomial $t^{\beta} \in F[t_i \mid i \in H] \subseteq A$ where $\beta \in \mathbb{N}^{\oplus H}$ is mapped to $1/(s - a)^{\beta}$. Recall that we aim to prove the surjectivity of φ: Given $p/q \in F[s]$, write p/q in the form above and pick up α and $\beta \in \mathbb{N}^{\oplus H}$ such that $k_i = \alpha_i - \beta_i$ for any $i \in H$ (and $\alpha_i = 0 = \beta_i$ for $k_i = 0$). Then we find polynomials $f := \lambda \prod_i (t_j - a_i)^{\alpha_i} \in F[t_j] \subseteq A$ and $g := t^{\beta} \in F[t_i \mid i \in H] \subseteq A$ such that $fg \in A$ is mapped to $p/q \in F(s)$ under φ, since

$$
\varphi\left(\lambda \prod_{i \in H} (t_j - a_i)^{\alpha_i} \cdot t^{\beta} \right) \; = \; \lambda \prod_{i \in H} (s - a_i)^{\alpha_i} \cdot \frac{1}{(s - a)^{\beta}} \; = \; \lambda \prod_{i \in H} \frac{(s - a_i)^{\alpha_i}}{(s - a_i)^{\beta_i}} \; = \; \frac{p(s)}{q(s)}
$$

As p/q have been arbitrary φ is surjective and if we let $\mathfrak{m} := \ker(\varphi)$ we therefore find an isomorphism

$A/\mathfrak{m} \xrightarrow{\sim} F(s)$. As $F(s)$ is a field, $\mathfrak{m}$ is a maximal ideal. Now by (d) we find $\mathfrak{m} = \mathfrak{m}_x$ for some $x \in F^I$, in particular $t_i - x_i \in \mathfrak{m}$ for some $i \in H$. By construction this means

$$0 \;=\; \varphi(t_i - x_i) \;=\; \frac{1}{s - a_i} - x_i \;=\; \frac{1 - x_i s + x_i a_i}{s - a_i}$$

This yields $1 - x_i s + x_i a_i = 0$ and by comparing the coefficients of this polynomial in s, we get $x_i = 0$ and $0 = 1 + x_i a_i = 1$. But $0 = 1$ is an obvious contradiction to the assumption $|F| \leq |I|$.

□

Proof of (8.62):
By assumption F satisfies property (a) in theorem (8.60). So if we start with $\mathfrak{a} \in \operatorname{Srad}(A)$ then by property (i) in (8.60) we get $\mathbb{IV}(\mathfrak{a}) = \sqrt{\mathfrak{a}} = \mathfrak{a}$. Conversely if $X = \mathbb{V}(\mathfrak{a})$ is an algebraic set, then $\mathbb{I}(X)$ is a radical ideal, as any field is reduced. And due to the Galois connection property we get $\mathbb{VI}(X) = \mathbb{VIV}(\mathfrak{a}) = \mathbb{V}(\mathfrak{a}) = X$. In effect $\mathbb{V}$ and $\mathbb{I}$ are well-defined and mutually inverse maps.

If F is not algebraically closed, then property (b) in (8.60) has to fail, according to (8.58.(ii)). That is (d) has to fail and hence there are maximal ideals of A that do not correspond to a point $x \in F^I$. And if $|F| \leq |I|$, then we would be able to construct a maximal ideal $\mathfrak{m} \trianglelefteq_{\mathfrak{i}} A$ such that $\mathbb{V}(\mathfrak{m}) = \emptyset = \mathbb{V}(A)$, as we have seen in the proof of (b) $\implies$ (a) of theorem (8.60). Thus the correspondence fails in this case, too. □

Proof of (8.63):

(i) For any $x \in R^J$ let us abbreviate $\check{x} := \pi_I^J(x)$ and $\widehat{\mathfrak{a}} := \mathfrak{a}\,R[J]$. Then we start by decoding what it means that $x \in (\pi_I^J)^{-1}(\mathbb{V}(\mathfrak{a}))$. First of all this is $\check{x} \in \mathbb{V}(\mathfrak{a})$ and this again means $a(\check{x}) = 0$ for any $a \in \mathfrak{a}$. That is we have to prove that the following equivalence holds for all $x \in R^J$

$$\forall\, f \in \widehat{\mathfrak{a}} : f(x) = 0 \quad\Longleftrightarrow\quad \forall\, a \in \mathfrak{a} : a(\check{x}) = 0$$

In the direction " $\Longleftarrow$ " we are given some $a \in \mathfrak{a}$ and need to show that $a(\check{x}) = 0$. But letting $f = \widehat{a} := \iota_I^J(a) \in \mathfrak{a}\,R[J] = \widehat{\mathfrak{a}}$, this becomes apparent

$$a(\check{x}) \;=\; f(x) \;=\; 0$$

For the converse implication we are given $f \in \widehat{\mathfrak{a}}$ and need to show $f(x) = 0$. That is there are $f_i \in R[J]$ and $a_i \in \mathfrak{a}$ such that for $\widehat{a}_i := \iota_I^J(a_i)$ we get $f = f_1\,\widehat{a}_1 + \cdots + f_r\,\widehat{a}_r$. As above, it is clear, that $\widehat{a}_i(x) = a_i(\check{x})$ and hence

$$f(x) \;=\; f_1(x)\,a_1(\check{x}) + \cdots + f_r(x)\,a_r(\check{x}) \;=\; 0$$

(ii) Let us denote $\widehat{X} := (\pi_I^J)^{-1}(X) \subseteq R^J$ then we have to show $\mathbb{I}(\widehat{X}) = \mathbb{I}(X)\,R[J]$. For $I = J$ we have $\widehat{X} = X$ and $\mathbb{I}(X)\,R[J] = \mathbb{I}(X)$ so the claim is satisfied trivially. Also, in case $X = \emptyset$ we have $\widehat{X} = \emptyset$ and $\mathbb{I}(X) = \mathbb{I}(\emptyset) = R[I]$ such that $\mathbb{I}(\widehat{X}) = R[J] = \mathbb{I}(X)\,R[J]$. Thus we only need to consider $I \subset J$ and $X \neq \emptyset$. We first deal with the inclusion $\mathbb{I}(X)\,R[J] \subseteq \mathbb{I}(\widehat{X})$: As $\mathbb{I}(X)\,R[J]$ is generated by $\{\, \widehat{a} \mid a \in \mathbb{I}(X) \,\}$, where $\widehat{a} := \iota_I^J(a)$, it suffices to show $\widehat{a} \in \mathbb{I}(\widehat{X})$ for any $a \in \mathbb{I}(X)$.

But by construction $\widehat{a}(x) = a(\check{x}) = 0$ for any $x \in \widehat{X}$ with $\check{x} := \pi_I^J(x) \in X$. Thus we have

$$\mathbb{I}(X)\, R[J] \quad \subseteq \quad \mathbb{I}\big(\widehat{X}\big)$$

For the converse inclusion we have to regard any $f \in R[J]$ such that for any $x \in \widehat{X}$ we get $f(x) = 0$ and have to show $f \in \mathbb{I}(X)\, R[J]$. Fix any $\check{x} \in X$ and any $y \in R^{J \setminus I}$ then $x := (\check{x}, y) \in \widehat{X}$ and thereby $f(x) = 0$. Let $S := R[I]$ and $H := J \setminus I$. Note that $H \neq \emptyset$, as $I \subset J$. Then we write $f \in R[J]$ as a polynomial in $f \in S[H]$, that is

$$f \;=\; \sum_{(\alpha,\beta) \in \mathbb{N}^{\oplus J}} f[\alpha,\beta]\, t^{(\alpha,\beta)} \;=\; \sum_{\beta \in \mathbb{N}^{\oplus H}} \left(\sum_{\alpha \in \mathbb{N}^{\oplus I}} f[\alpha,\beta]\, t^{\alpha} \right) t^{\beta}$$

Then we turn our attention to $g(t) := f(\check{x}, t) \in R[H]$. By assumption on f we have $g(y) = f(x) = 0$ for any $y \in R^H$. And as R is an infinite integral domain this means $g = 0$. That is for any $\beta \in \mathbb{N}^{\oplus H}$ we have $f_\beta(\check{x}) = 0$ where

$$f_\beta \;:=\; \sum_{\alpha \in \mathbb{N}^{\oplus I}} f[\alpha,\beta]\, t^{\alpha} \;\in\; R[I]$$

As $\check{x} \in X$ has been arbitrary, this means $f_\beta \in \mathbb{I}(X)$. But by construction there are finitely many $\beta \in \mathbb{N}^{\oplus H}$ such that f can be written as $f = \sum_\beta f_\beta\, t^\beta$. Then, as any $f_\beta \in \mathbb{I}(X)$ we get $f \in \mathbb{I}(X)\, R[J]$ and thereby we also have the converse inclusion.

(iii) The inclusion $\sqrt{\mathfrak{u}} \subseteq \mathbb{I}\,\mathbb{V}(\mathfrak{u})$ is generally true, for any reduced ring R. For the converse inclusion note that any algebraically closed field already is an infinite integral domain. By (i) we have $\mathbb{V}(\mathfrak{u}) = (\pi_I^J)^{-1}(\mathbb{V}(\mathfrak{a}))$ and (ii) turns this into

$$\begin{aligned} \mathbb{I}\,\mathbb{V}(\mathfrak{u}) \;&=\; \mathbb{I}\left(\left(\pi_I^J\right)^{-1} (\mathbb{V}(\mathfrak{a})) \right) \;=\; \mathbb{I}\,\mathbb{V}(\mathfrak{a})\, R[J] \\ &=\; \sqrt{\mathfrak{a}}\, R[J] \;\subseteq\; \sqrt{\mathfrak{a}\, R[J]} \;=\; \sqrt{\mathfrak{u}} \end{aligned}$$

□

8.6 Galois Theory

8.7 Krull Dimension

The notion of the dimension of a commutative ring is inspired by algebraic geometry: E.g. a flying carpet is a 2-dimensional object, this can be seen in two ways: (1) at any point, the tangential space is a plane or (2) we can build up the dimension iteratively: The flying carpet contains the image of a plane, which contains the image of a line, which contains the image of a point. As in each step the dimension is increased by 1 and as we start with dimension 0 (of a point), we end up at 2 again. Hence in algebraic geometry (without going into details), the dimension can be defined by chains of irreducible subsets - the longer the chain can be, the higher the dimension. As prime ideals correspond to irreducible subsets (in a order-reversing way), we can measure the length of the chain in the ring of regular functions of the variety. The theory we are about to present here is about lengths of chains of prime ideals, as they can be better controlled, than irreducible subsets. It will be the perfect tool for algebraic geometry.

This sub-section boasts several theorems of great renown: After some preleminary results we provide going-up and down. We then compare the Krull dimension with the transcendence degree of an algebra, by continuing the Noetherian normalisation theorem. And finally we aim for Krulls principal ideal theorem, which gives an upper on the number of generators of an ideal in a noetherian ring. These theorems are hard-earned, step by step we wall in the truth until it finally cannot elude us any more. Alas, the sweetest fruits are the hardest to pluck.

(8.64) Definition:
Let $(R,+,\cdot)$ be a commutative ring, then a tuple $(\mathfrak{p}_0,\ldots,\mathfrak{p}_n)$ is said to be a **chain of prime ideals** (which we usually abbreviate by **CPI** iff it satisfies the following properties (1), (2) and (3), where

(1) For any $k \in 0\ldots n$ $\mathfrak{p}_k \trianglelefteq_{\mathfrak{i}} R$ is a prime ideal

(2) For any $k \in 1\ldots n$ we have $\mathfrak{p}_{k-1} \subseteq \mathfrak{p}_k$

(3) For any $k \in 1\ldots n$ we have $\mathfrak{p}_{k-1} \neq \mathfrak{p}_k$

We denote the set of all chains of prime ideals in R by $\mathrm{CPI}(R)$. An if $\mathfrak{p}$ and $\mathfrak{q}$ are prime ideals of R, then the set of all chains of prime ideals that start in $\mathfrak{p}$ is denoted by $\mathrm{CPI}_{\mathfrak{p}}(R)$. The set of all chains of prime ideals that end in $\mathfrak{q}$ is denoted by $\mathrm{CPI}^{\mathfrak{q}}(R)$. Formally

$$\begin{aligned}
\mathrm{CPI}(R) &:= \{\,(\mathfrak{p}_0,\ldots,\mathfrak{p}_n) \mid (1),(2),(3)\,\}\\
\mathrm{CPI}_{\mathfrak{p}}(R) &:= \{\,(\mathfrak{p}_0,\ldots,\mathfrak{p}_n) \in \mathrm{CPI}(R) \mid \mathfrak{p}_0 = \mathfrak{p}\,\}\\
\mathrm{CPI}^{\mathfrak{q}}(R) &:= \{\,(\mathfrak{p}_0,\ldots,\mathfrak{p}_n) \in \mathrm{CPI}(R) \mid \mathfrak{p}_n = \mathfrak{q}\,\}\\
\mathrm{CPI}^{\mathfrak{q}}_{\mathfrak{p}}(R) &:= \{\,(\mathfrak{p}_0,\ldots,\mathfrak{p}_n) \in \mathrm{CPI}(R) \mid \mathfrak{p}_0 = \mathfrak{p} \text{ and } \mathfrak{p}_n = \mathfrak{q}\,\}
\end{aligned}$$

Finally, if $\mathcal{P} = (\mathfrak{p}_0,\ldots,\mathfrak{p}_m)$ and $\mathcal{Q} = (\mathfrak{q}_0,\ldots,\mathfrak{q}_n) \in \mathrm{CPI}(R)$ are any two chains of prime ideals in R, then we introduce a partial order $\leq$ on $\mathrm{CPI}(R)$, by letting $\mathcal{P} \leq \mathcal{Q}$, iff one of the following two equivalent conditions is satisfied

(a) $\{\,\mathfrak{p}_0,\ldots,\mathfrak{p}_m\,\} \subseteq \{\,\mathfrak{q}_0,\ldots,\mathfrak{q}_n\,\}$

(b) $\exists\, j : 0\ldots m \hookrightarrow 0\ldots n$ injective, such that $\forall\, i \in 0\ldots m$ we get $\mathfrak{p}_i = \mathfrak{q}_{j(i)}$

Prob If (a) then any $\mathfrak{p}_i \in \{\, \mathfrak{q}_0, \ldots, \mathfrak{q}_n \,\}$. That is there is some $j(i) \in 0 \ldots n$ such that $p_i \in \mathfrak{q}_{j(i)}$. And as the $\mathfrak{p}_i$ are pairwise distinct, by (3), the map $j : i \mapsto j(i)$ is injective. So we got (b). If conversely (b) then for any $i \in 0 \ldots m$ we get $\mathfrak{p}_i = \mathfrak{q}_{j(i)} \in \{\, \mathfrak{q}_0, \ldots, \mathfrak{q}_n \,\}$, which is (a). Thereby it is clear, that $\leq$ inherits the properties of a partial order from $\subseteq$ in property (a).

(8.65) Remark:

(i) Consider a commutative ring $(R, +, \cdot)$ and a prime ideal $\mathfrak{p} \in \operatorname{Spec}(R)$. By the correspondence theorem of prime ideals (1.71) the prime ideals of $R/\mathfrak{p}$ correspond to the prime ideals of R that contain $\mathfrak{p}$. And as this correspondence respects the inclusion $\subseteq$ it is clear, that we get the following one-to-one correspondence of chains of prime ideals

$$\begin{array}{rcl} \{\, \mathcal{P} \in \operatorname{CPI}(R) \mid \mathfrak{p} \subseteq \mathfrak{p}_0 \,\} & \longleftrightarrow & \operatorname{CPI}\left(R \Big/ \mathfrak{p}\right) \\ \mathcal{P} = (\mathfrak{p}_0, \ldots, \mathfrak{p}_n) & \mapsto & \left(\mathfrak{p}_0 \Big/ \mathfrak{p}, \ldots, \mathfrak{p}_n \Big/ \mathfrak{p}\right) \end{array}$$

(ii) Likewise by (2.129) there is a one to one correspondence between the prime ideals of the localisation $R_\mathfrak{p}$ and the prime ideals of R that are contained in $\mathfrak{p}$, where $\mathfrak{p}_k R_\mathfrak{p} = \{\, a/u \in R_\mathfrak{p} \mid a \in \mathfrak{p}_k, u \in R \setminus \mathfrak{p} \,\}$. Recall that $R_\mathfrak{p}$ is a local ring with maximal ideal $\mathfrak{p}R_\mathfrak{p}$ according to (2.138). This correspondence also respects inclusions and hence grants a one-to-one correspondence of chains of prime ideals

$$\begin{array}{rcl} \{\, \mathcal{P} \in \operatorname{CPI}(R) \mid \mathfrak{p}_n \subseteq \mathfrak{p} \,\} & \longleftrightarrow & \operatorname{CPI}(R_\mathfrak{p}) \\ \mathcal{P} = (\mathfrak{p}_0, \ldots, \mathfrak{p}_n) & \mapsto & (\mathfrak{p}_0 R_\mathfrak{p}, \ldots, \mathfrak{p}_n R_\mathfrak{p}) \end{array}$$

(iii) Let us combine (i) and (ii): If $\mathfrak{p} \subseteq \mathfrak{q} \in \operatorname{Spec}(R)$ are nested primes of R, then we take $Q := R/\mathfrak{p}$ a quotient ring of R, that is an integral domain. By (i) $\overline{\mathfrak{q}} := \mathfrak{q}/\mathfrak{p}$ is a prime ideal in Q and thereby we can take to the local ring $Q_{\overline{\mathfrak{q}}}$ whose maximal ideal is given to be $\overline{\mathfrak{q}} Q_{\overline{\mathfrak{q}}}$. And we obtain a one-to-one correspondence of chains of prime ideals

$$\begin{array}{rcl} \operatorname{CPI}^{\mathfrak{q}}_{\mathfrak{p}}(R) & \longleftrightarrow & \operatorname{CPI}(Q_{\overline{\mathfrak{q}}}) \\ (\mathfrak{p}_0, \ldots, \mathfrak{p}_n) & \mapsto & \left(\mathfrak{p}_0 \Big/ \mathfrak{p}Q_{\overline{\mathfrak{q}}}, \ldots, \mathfrak{p}_n \Big/ \mathfrak{p}Q_{\overline{\mathfrak{q}}}\right) \end{array}$$

(8.66) Definition: (viz. 1271)
Let $(R, +, \cdot)$ be a commutative ring again, then a CPI $(\mathfrak{p}_0, \ldots, \mathfrak{p}_m)$ of R is said to be **saturated**, iff it cannot be extended to a longer chain by inserting more prime ideals. That is iff it satisfies one of the following two conditions

(a) The chain $(\mathfrak{p}_0, \ldots, \mathfrak{p}_m)$ is a maximal element of $\operatorname{CPI}^{\mathfrak{q}}_{\mathfrak{p}}(R)$, where $\mathfrak{p} = \mathfrak{p}_0$ and $\mathfrak{q} = \mathfrak{p}_m$. That is for any CPI $(\mathfrak{q}_0, \ldots, \mathfrak{q}_n)$ that satisfies $\mathfrak{q}_0 = \mathfrak{p}_0$ and $\mathfrak{q}_n = \mathfrak{p}_m$ we get

$$(\mathfrak{p}_0, \ldots, \mathfrak{p}_m) \leq (\mathfrak{q}_0, \ldots, \mathfrak{q}_n) \quad \Longrightarrow \quad (\mathfrak{p}_0, \ldots, \mathfrak{p}_m) = (\mathfrak{q}_0, \ldots, \mathfrak{q}_n)$$

(b) For any prime ideal $\mathfrak{p} \in \operatorname{Spec}(R)$ and any index $k \in 1 \ldots m$ we have the following implication

$$\mathfrak{p}_{k-1} \subseteq \mathfrak{p} \subseteq \mathfrak{p}_k \quad \Longrightarrow \quad \mathfrak{p}_{k-1} = \mathfrak{p} \text{ or } \mathfrak{p} = \mathfrak{p}_k$$

And $(\mathfrak{p}_0, \ldots, \mathfrak{p}_m)$ is said to be **maximal**, iff it cannot be extended to a longer chain by inserting or appending prime ideals at any position. That is iff it satisfies one of the following two conditions

(a) The chain $(\mathfrak{p}_0, \ldots, \mathfrak{p}_m)$ is a maximal element of $\mathrm{CPI}(R)$. That is for any CPI $(\mathfrak{q}_0, \ldots, \mathfrak{q}_n)$ we get

$$(\mathfrak{p}_0, \ldots, \mathfrak{p}_m) \leq (\mathfrak{q}_0, \ldots, \mathfrak{q}_n) \quad \Longrightarrow \quad (\mathfrak{p}_0, \ldots, \mathfrak{p}_m) = (\mathfrak{q}_0, \ldots, \mathfrak{q}_n)$$

(b) The chain $(\mathfrak{p}_0, \ldots, \mathfrak{p}_m)$ satisfies the following three properties: (1) it is saturated, (2) $\mathfrak{p}_m$ is a maximal ideal of R and (3) $\mathfrak{p}_0$ is a minimal prime ideal of R. That is for any prime ideal $\mathfrak{p} \in \mathrm{Spec}(R)$ we get $\mathfrak{p} \subseteq \mathfrak{p}_0 \implies \mathfrak{p} = \mathfrak{p}_0$.

(8.67) Remark:
If $(R, +, \cdot)$ is any commutative ring $\mathfrak{p}$ and $\mathfrak{q} \in \mathrm{Spec}(R)$ are prime ideals and $\mathcal{Q} = (\mathfrak{q}_0, \ldots, \mathfrak{q}_n)$ is a CPI of R, with $\mathfrak{p} = \mathfrak{q}_0$ and $\mathfrak{q}_n = \mathfrak{q}$. If $\mathcal{P}$ is of maximal length with this property, that is

$$\ell(\mathcal{Q}) \quad = \quad \max\{\, \ell(\mathcal{P}) \in \mathbb{N} \mid \exists\, \mathcal{P} \in \mathrm{CPI}_{\mathfrak{p}}^{\mathfrak{q}}(R) \,\}$$

Then $\mathcal{Q}$ obviously is saturated, as any CPI that truly extends $\mathcal{Q}$ would have to exceed $\mathcal{Q}$ in length. The converse need not be true, however: There may be CPI from $\mathfrak{p}$ to $\mathfrak{q}$ that are longer than a given saturated CPI. Counter-examples are not easy to find, but Nagata managed to do so.

(8.68) Definition:
Once more let $(R, +, \cdot)$ be a commutative ring and $\mathcal{P} = (\mathfrak{p}_0, \ldots, \mathfrak{p}_n)$ be a CPI in R. Then we call n the **length** of $\mathcal{P}$ and denote it by $\ell(\mathcal{P}) := n$. Now if $R \neq 0$ is non-zero, then we define its **Krull-dimension** [or simply its *dimension*] to be the maximal length of any CPI contained in R. If the length is unbound, then the dimension of R is infinite, formally

$$\mathrm{kdim}(R) \quad := \quad \sup\{\, \ell(\mathcal{P}) \mid \mathcal{P} \in \mathrm{CPI}(R) \,\} \quad \in \quad \mathbb{N} \cup \{\infty\}$$

If $R \neq 0$, then $\mathrm{kdim}(R) \geq 0$, as there always is at least one maximal ideal contained in R. And in case $R = 0$ we specifically define $\mathrm{kdim}(R) := -1$. And for a fixed prime ideal $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$, we define the **height** of $\mathfrak{p}$ to be the maximal length of a CPI, that terminates in $\mathfrak{p}$:

$$\mathrm{height}(\mathfrak{p}) \quad := \quad \sup\{\, \ell(\mathcal{P}) \mid \mathcal{P} \in \mathrm{CPI}^{\mathfrak{p}}(R) \,\} \quad \in \quad \mathbb{N} \cup \{\infty\}$$

For the ideal $\mathfrak{a} = R$ we specifically define $\mathrm{height}(R) = -1$. And for a proper ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ (that is $\mathfrak{a} \neq R$) there is a maximal ideal containing $\mathfrak{a}$, according to (2.4.(ii)) and hence we may define the **height** of $\mathfrak{a}$ to be the minimal height of a prime ideal containing $\mathfrak{a}$.

$$\mathrm{height}(\mathfrak{a}) \quad := \quad \inf\{\, \mathrm{height}(\mathfrak{p}) \mid \mathfrak{p} \in \mathrm{Spec}(R) \ \text{ with } \mathfrak{a} \subseteq \mathfrak{p} \,\} \quad \in \quad \mathbb{N} \cup \{\infty\}$$

Nota if $\mathfrak{a} = \mathfrak{p}$ is a prime ideal of R itself, then $\mathrm{height}(\mathfrak{a})$ in this sense equals $\mathrm{height}(\mathfrak{p})$ as a prime ideal. This is clear, as any prime ideal $\mathfrak{q}$ with $\mathfrak{a} \subseteq \mathfrak{q}$ already contains $\mathfrak{p} \subseteq \mathfrak{q}$ and hence $\mathrm{height}(\mathfrak{p}) \leq \mathrm{height}(\mathfrak{q})$. In case of doubt refer to (8.69.(vi)) below.

Nota recall the notation $\mathbb{V}(\mathfrak{a}) := \{\, \mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{a} \subseteq \mathfrak{p} \,\}$, which is a non-epmty set, as $\mathfrak{a} \neq R$. Using this we can rewrite the above definition, as $\mathrm{height}(\mathfrak{a}) = \min\{\, \mathrm{height}(\mathfrak{p}) \mid \mathfrak{p} \in \mathbb{V}(\mathfrak{a}) \,\}$. Some authors only allow prime ideals minimal over $\mathfrak{a}$, that is they define $\mathrm{height}(\mathfrak{a}) = \min\{\, \mathrm{height}(\mathfrak{p}) \mid \mathfrak{p} \in \mathbb{V}(\mathfrak{a})_* \,\}$. But we will see in (8.69.(vii)) below, that both definitions return the same result.

(8.69) Proposition: (viz. 1236)
Let $(R, +, \cdot)$ be any commutative ring and $\mathfrak{p} \in \mathrm{Spec}(R)$ be any prime ideal of R. Then the following statements are generally true

(i) If $\mathcal{P} \in \mathrm{CPI}(R)$ is a chain of prime ideals with $\ell(\mathcal{P}) = \mathrm{kdim}(R)$, then $\mathcal{P}$ is maximal.

(ii) If $(S, +, \cdot)$ is another commutative ring and $\varphi : S \twoheadrightarrow R$ is a surjective homomorphism of rings, then the Krull-dimension of R cannot exceed the Krull-dimension of S, that is

$$\mathrm{kdim}(R) \quad \leq \quad \mathrm{kdim}(S)$$

Nota If $\varphi : R \hookrightarrow S$ is an injective homomorphism of rings, than we cannot draw this conclusion. An easy counter-example is $\mathbb{Z} \hookrightarrow \mathbb{Q}$ where we have $\mathrm{kdim}(\mathbb{Z}) = 1 > 0 = \mathrm{kdim}(\mathbb{Q})$.

(iii) Any prime ideal $\mathfrak{p} \in \mathrm{Spec}(R)$ is a minimal prime (that is for any other $\mathfrak{p}' \in \mathrm{Spec}(R)$ we have the implication $\mathfrak{p}' \subseteq \mathfrak{p} \implies \mathfrak{p}' = \mathfrak{p}$) if and only if, it has $\mathrm{height}(\mathfrak{p}) = 0$. Formally that is

$$\mathrm{Smin}(R) \quad = \quad \{\, \mathfrak{p} \in \mathrm{Spec}(R) \mid \mathrm{height}(\mathfrak{p}) = 0 \,\}$$

(iv) The Krull-dimension of $R/\mathrm{nil}(R)$ equals the Krull-dimension of R, that is we have the identity

$$\mathrm{kdim}\left(R \Big/ \mathrm{nil}(R) \right) \quad = \quad \mathrm{kdim}(R)$$

(v) By definition the dimension of R is the maximal height of a prime ideal of R. But this definition already yields the following identities

$$\begin{aligned} \mathrm{kdim}(R) \quad &= \quad \sup\{\, \mathrm{height}(\mathfrak{a}) \mid \mathfrak{a} \in \mathrm{Ideal}(R) \,\} \\ &= \quad \sup\{\, \mathrm{height}(\mathfrak{p}) \mid \mathfrak{p} \in \mathrm{Spec}(R) \,\} \\ &= \quad \sup\{\, \mathrm{height}(\mathfrak{m}) \mid \mathfrak{m} \in \mathrm{Smax}(R) \,\} \end{aligned}$$

(vi) If $\mathfrak{p}$, $\mathfrak{q}$ are any prime ideals of R with $\mathrm{height}(\mathfrak{q}) < \infty$ then we get the following implication

$$\mathfrak{p} \subset \mathfrak{q} \quad \Longrightarrow \quad \mathrm{height}(\mathfrak{p}) < \mathrm{height}(\mathfrak{q})$$

(vii) Let $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be any ideal and $\mathfrak{p} \in \mathrm{Spec}(R)$ be a prime ideal of R, such that $\mathfrak{a} \subseteq \mathfrak{p}$ and $\mathrm{height}(\mathfrak{a}) = \mathrm{height}(\mathfrak{p})$. Then $\mathfrak{p}$ already is a *minimal over* $\mathfrak{a}$ [that is for any $\mathfrak{p}' \in \mathrm{Spec}(R)$ with $\mathfrak{a} \subseteq \mathfrak{p}' \subseteq \mathfrak{p}$ we get $\mathfrak{p}' = \mathfrak{p}$]. Therefore, if $\mathfrak{a} \neq R$ is a proper ideal of finite height $\mathrm{height}(\mathfrak{a}) < \infty$, then we get

$$\mathrm{height}(\mathfrak{a}) \quad = \quad \min\{\, \mathrm{height}(\mathfrak{p}) \mid \mathfrak{a} \subseteq \mathfrak{p} \text{ minimal over } \mathfrak{a} \,\}$$

(viii) Let $\mathfrak{p}$, $\mathfrak{q} \in \operatorname{Spec}(R)$ be prime ideals and recall the notion that $\mathfrak{p}$ lies *directly under* $\mathfrak{q}$ iff (1) $\mathfrak{p} \subset \mathfrak{q}$ and (2) for any $\mathfrak{p}' \in \operatorname{Spec}(R)$ with $\mathfrak{p} \subseteq \mathfrak{p}' \subseteq \mathfrak{q}$ we get $\mathfrak{p}' = \mathfrak{p}$ or $\mathfrak{p}' = \mathfrak{q}$. We denote this by writing $\mathfrak{p} \subset_* \mathfrak{q}$. If now $(\mathfrak{p}_0, \ldots, \mathfrak{p}_n)$ is a CPI of R, such that $n = \operatorname{kdim}(R)$, then we have

(1) $\mathfrak{p}_0 \in \operatorname{Smin}(R)$ and $\mathfrak{p}_n \in \operatorname{Smax}(R)$

(2) $\forall\, k \in 1 \ldots n : \mathfrak{p}_{k-1} \subset_* \mathfrak{p}_k$

(3) $\forall\, k \in 0 \ldots n : \operatorname{height}(\mathfrak{p}_k) = k$

Likewise, if $(\mathfrak{p}_0, \ldots, \mathfrak{p}_r)$ is a CPI of R such that $r = \operatorname{height}(\mathfrak{p}_r)$, then we get the following properties:

(1) $\mathfrak{p}_0 \in \operatorname{Smin}(R)$

(2) $\forall\, k \in 1 \ldots r : \mathfrak{p}_{k-1} \subset_* \mathfrak{p}_k$

(3) $\forall\, k \in 0 \ldots r : \operatorname{height}(\mathfrak{p}_k) = k$

(ix) The height of $\mathfrak{p}$ in R equals the Krull-dimension of $R_{\mathfrak{p}}$ as a ring, that is we have the identity

$$\operatorname{kdim}(R_{\mathfrak{p}}) \quad = \quad \operatorname{height}(\mathfrak{p})$$

(x) If R is finite-dimensional, then so are the quotient ring $R/\mathfrak{p}$ and localisation $R_{\mathfrak{p}}$. More generally, for any ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ we have the following estimate of dimensions

$$\operatorname{kdim}\left(R \Big/ \mathfrak{a}\right) + \operatorname{height}(\mathfrak{a}) \quad \leq \quad \operatorname{kdim}(R)$$

(xi) Let $\mathfrak{q} \subseteq \mathfrak{q}$ are nested prime ideals of R, such that $\operatorname{height}(\mathfrak{q}) < \infty$ is finite. If we then regard $\mathfrak{q}/\mathfrak{p}$ as a prime ideal in the quotient ring $R/\mathfrak{p}$, we find the following estimate

$$\operatorname{height}\left(\mathfrak{q} \Big/ \mathfrak{p}\right) \quad \leq \quad \operatorname{height}(\mathfrak{q}) - \operatorname{height}(\mathfrak{p})$$

(xii) If now $\mathfrak{q}$ is a prime ideal of R, such that $1 \leq \operatorname{height}(\mathfrak{q}) < \infty$, then the height of $\mathfrak{q}$ is one step above the maximal height of any prime ideal lying directly under $\mathfrak{q}$. Formally put, that is

$$\operatorname{height}(\mathfrak{q}) \quad = \quad 1 + \max\{\, \operatorname{height}(\mathfrak{p}) \mid \mathfrak{p} \in \operatorname{Spec}(R) \text{ with } \mathfrak{p} \subset_* \mathfrak{q} \,\}$$

(xiii) Let $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be any ideal and $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ be a prime ideal, such that $\mathfrak{a} \subseteq \mathfrak{p}$. Also let $a \in \operatorname{NZD}(R)$ be a non-zero-divisor of R that is contained in $a \in \mathfrak{a}$. Then $\mathfrak{p}/\mathfrak{a}$ is a prime ideal in the quotient ring $R/\mathfrak{a}$ and either $\operatorname{height}(\mathfrak{p}/\mathfrak{a}) = \operatorname{height}(\mathfrak{p}) = \infty$ or the height of this ideal is less, than the height of $\mathfrak{p}$. The latter formally is

$$\operatorname{height}\left(\mathfrak{p} \Big/ \mathfrak{a}\right) \quad < \quad \operatorname{height}(\mathfrak{p})$$

(8.70) Example:

(i) If $(F, +, \cdot)$ is a field, then $\operatorname{kdim}(F) = 0$, as (0) is the one and only chain of prime ideals, that is available in F, at all. This will be generalized in (iii) below.

(ii) If $(R,+,\cdot)$ is a PID, but not a field, then $\mathrm{kdim}(R) = 1$. This can be seen in the following way: Suppose $\mathcal{P} = (\mathfrak{p}_0,\ldots,\mathfrak{p}_n)$ is a CPI of R with $n = \mathrm{kdim}(R)$. Then $\mathcal{P}$ is maximal and hence $\mathfrak{p}_0 = 0$, as this is the one and only minimal prime ideal of R. Now $\mathfrak{p}_k = p_k R$ for some prime elements $p_k \in R$. As $\mathfrak{p}_{k-1} \subseteq \mathfrak{p}_k$ we have $p_k \mid p_{k-1}$. But as p_{k-1} is prime this would mean $p_k \approx p_{k-1}$ by (2.58.(vi)). This again would be $\mathfrak{p}_{k-1} = \mathfrak{p}_k$ such that $n \geq 2$ is ruled out. Hence the CPI is $(0, p_1 R)$ at most and hence $1 = n = \mathrm{kdim}(R)$.

(iii) Any commutative ring $(R,+,\cdot)$ has $\mathrm{kdim}(R) = 0$ if and only if all of its prime ideals already are maximal. That is we have the following equivalence

$$\mathrm{kdim}(R) \;=\; 0 \quad\Longleftrightarrow\quad \mathrm{Spec}(R) \;=\; \mathrm{Smax}(R)$$

This equivalence can be seen in the following way: If $\mathrm{kdim}(R) = 0$ and $\mathfrak{p}$ is any prime ideal of R, then $\mathcal{P} = (\mathfrak{p})$ is a CPI with $\ell(\mathcal{P}) = 0 = \mathrm{kdim}(R)$. In particular $\mathcal{P}$ is a maximal CPI and hence $\mathfrak{p}$ is a maximal ideal. Conversely, if $\mathrm{Spec}(R) = \mathrm{Smax}(R)$, then in any CPI $(\mathfrak{p}_0,\ldots,\mathfrak{p}_n)$ of R, the first ideal $\mathfrak{p}_0$ is prime and hence maximal. But therefore there can be no $\mathfrak{p}_1$, only $n = 0$ and this means $\mathrm{kdim}(R) = 0$. Nota In the light of (2.37.(e)) this means: R is artinian if and only if R is a noetherian ring, with $\mathrm{kdim}(R) = 0$.

(iv) Consider the polynomial $t^5 \in \mathbb{C}[t]$ and let $R := \mathbb{C}[t]/t^5\mathbb{C}[t]$ be the quotient ring. Then the element $a := t^2 + t^5\mathbb{C}[t] \in R$ is a zero-divisor, as $(t^3 + t^5\mathbb{C}[t])(t^2 + t^5\mathbb{C}[t]) = 0$. Now $\mathfrak{p} := (t + t^5\mathbb{C}[t])R$ is a prime ideal of R, containing $a \in \mathfrak{p}$. But $\mathfrak{p}$ is a minimal prime in R and hence $\mathrm{height}(\mathfrak{p}) = 0$. This example shows, that zero-divisors do not have to contribute to the height of prime ideals.

(v) Being noetherian and being finite-dimensional are not necessary for one and another: That is non-noetherian rings may have finite Krull-dimension and noetherian rings may have infinite Krull-dimension. Here comes a cunning example (found by Nagata) of a ring, that is noetherian, but has infinite Krull-dimension. We only give a sketch of the construction here, more details on why it works out can be found at (■) https://math.stackexchange.com/questions/1109732/noetherian-ring-with- infinite-krull-dimension-nagatas-example.

Pick up any field F and let $A := F[t_1, t_2, \ldots]$ be the polynomial ring in countably many variables. Recursively define the indices $m(0) := 0$ and for $k \geq 1$ also $m(k) := m(k-1) + k$. That is $m(1) = 1$, $m(2) = 3$, $m(3) = 6$ and so on. Then for any $1 \leq k \in \mathbb{N}$ we take the prime ideal

$$\mathfrak{p}_k \;:= \langle t_j \mid m(k-1) < j \leq m(k) \rangle_{\mathrm{i}} \quad \trianglelefteq_{\mathrm{i}} \quad A$$

That is $\mathfrak{p}_1 = t_1 A$, $\mathfrak{p}_2 = t_2 A + t_3 A$, $\mathfrak{p}_3 = t_4 A + t_5 A + t_6 A$ and so on. As any $R \setminus \mathfrak{p}_k$ is multiplicatively closed, we obtain a multiplicatively closed subset U of A by intersection

$$U \;:=\; \bigcap_{k \geq 1} (R \setminus \mathfrak{p}_k)$$

The evil ring now is $R := U^{-1}A$. Then any $\mathfrak{m}_k := U^{-1}\mathfrak{p}_k$ is a maximal ideal of R, in fact these are all the maximal ideals of R. And the height of $\mathfrak{m}_k$ is given to be

$$\mathrm{height}(\mathfrak{m}_k) \;=\; m(k) - m(k-1) \;=\; k$$

This means R contains maximal ideals of unbounded height and therefore cannot have a finite Krull-dimension. Yet it can be proved that R is noetherian, as all the localisations $R_{\mathfrak{m}}$ for $\mathfrak{m} \in \mathrm{Smax}(R)$ are noetherian. Recall that is suffices to check this for all $\mathfrak{m} = \mathfrak{m}_k$.

(8.71) Remark:
Let $(R, +, \cdot)$ be a finite-dimensional ring. Note that $n = \mathrm{kdim}(R)$ means, that for any CPI $(\mathfrak{p}_0, \ldots, \mathfrak{p}_m)$ of R we have $m \leq n$. Therefore the following two statements are easy to see:

(i) If $\mathcal{P} \in \mathrm{CPI}(R)$ is a chain of prime ideals of R, then there already is a chain $\mathcal{P}^* \in \mathrm{CPI}(R)$ of prime ideals, that is maximal and extends $\mathcal{P} \leq \mathcal{P}^*$.

(ii) If $\mathfrak{p} \subseteq \mathfrak{q} \in \mathrm{Spec}(R)$ are any two nested primes of R and $\mathcal{P} \in \mathrm{CPI}^{\mathfrak{q}}_{\mathfrak{p}}(R)$ is a chain of prime ideals of R, then there already is a chain $\mathcal{P}^* \in \mathrm{CPI}^{\mathfrak{q}}_{\mathfrak{p}}(R)$ that is saturated and extends $\mathcal{P} \leq \mathcal{P}^*$.

Prob If $\mathcal{P}$ is maximal itself, then we are done. Otherwise there is some $\mathcal{P}_1 \in \mathrm{CPI}(R)$ with $\mathcal{P} < \mathcal{P}_1$. In particular $\ell(\mathcal{P}) < \ell(\mathcal{P}_1) \leq \mathrm{kdim}(R)$. If $\mathcal{P}_1$ is maximal, we are done, otherwise we continue with $\mathcal{P}_1$ and pick up $\mathcal{P}_2$ with $\mathcal{P}_1 < \mathcal{P}_2$ and so on. This can be done at most $m \leq \mathrm{kdim}(R) - \ell(\mathcal{P})$ times, so with $\mathcal{P}_m$ we cannot continue. But this happens only if $\mathcal{P}_m$ is maximal and we have $\mathcal{P} \leq \mathcal{P}_m$ by construction. The reasoning for (ii) is literally the same if you replace $\mathrm{CPI}(R)$ by $\mathrm{CPI}^{\mathfrak{q}}_{\mathfrak{p}}(R)$ and *maximal* with *saturated*.

(8.72) Lemma: (viz. 1240)

(i) *Lying-over Theorem*: If $S : R$ is an integral ring extension and $\mathfrak{q}_0 \subset \ldots \subset \mathfrak{q}_r$ is a CPI of S, then the pull-back $\mathfrak{q}_0 \cap R \subset \ldots \subset \mathfrak{q}_r \cap R$ is a CPI of R, as well.

(ii) *Going-up Theorem*: If $S : R$ is an integral ring extension, $\mathfrak{p}_0 \subset \ldots \subset \mathfrak{p}_r$ is a CPI of R and $\mathfrak{q}_0 \in \mathrm{Spec}(S)$ is a prime ideal in S such that $\mathfrak{q}_0 \cap R = \mathfrak{p}_0$, then there is $\mathfrak{q}_0 \subset \ldots \subset \mathfrak{q}_r$ a CPI of S such that we get $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ for any $i \in 1 \ldots r$.

(iii) *Going-down Theorem*: Let $S : R$ be an integral ring extension, such that R is a normal domain and S is torsion-free, as an R module. Now consider $\mathfrak{p}_0 \subset \ldots \subset \mathfrak{p}_r$ a CPI of R and $\mathfrak{q}_r \in \mathrm{Spec}(S)$ a prime ideal in S such that $\mathfrak{q}_r \cap R = \mathfrak{p}_r$, then there is $\mathfrak{q}_0 \subset \ldots \subset \mathfrak{q}_r$ a CPI of S such that we get $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ for any $i \in 1 \ldots r$.

(8.73) Corollary: (viz. 1244)

(i) Let $S : R$ be an integral ring extension, then R and S share the same Krull dimension, formally

$$\mathrm{kdim}(R) \;=\; \mathrm{kdim}(S)$$

(ii) If $S : R$ is an integral ring extension and $\mathfrak{u} \trianglelefteq_{\mathfrak{i}} S$ is any ideal of S, then we also find the following identity of Krull-dimensions

$$\mathrm{kdim}\left(S \big/ \mathfrak{u}\right) \;=\; \mathrm{kdim}\left(R \big/ \mathfrak{u} \cap R\right)$$

(iii) If $S : R$ is an integral ring extension and $\mathfrak{u} \trianglelefteq_{\mathrm{i}} S$ is any ideal of S, then the height of $\mathfrak{u} \cap R$ cannot exceed the height of $\mathfrak{u}$ that is we have the inequality

$$\operatorname{height}\big(\mathfrak{u} \cap R\big) \;\leq\; \operatorname{height}\big(\mathfrak{u}\big)$$

(iv) Let $S : R$ be an integral ring extension, such that R is a normal domain and S is torsion-free, as an R-module. If now $\mathfrak{q} \trianglelefteq_{\mathrm{i}} S$ is any prime ideal of S, then we even get

$$\operatorname{height}\big(\mathfrak{q} \cap R\big) \;=\; \operatorname{height}\big(\mathfrak{q}\big)$$

(8.74) Definition:

(i) A commutative ring $(R, +, \cdot)$ is said to be **holodimensional** if $\operatorname{kdim}(R) < \infty$ it has finite Krull-dimension and for any chain of prime ideals $\mathcal{P} \in \mathrm{CPI}(R)$ of R we get the equivalence

$$\mathcal{P} \text{ is maximal} \iff \ell(\mathcal{P}) = \operatorname{kdim}(R)$$

(ii) A commutative ring $(R, +, \cdot)$ is said to be **equidimensional** if $\operatorname{kdim}(R) < \infty$ it has finite Krull-dimension and any two maximal ideals $\mathfrak{m}, \mathfrak{n} \in \operatorname{Smax}(R)$ have the same height, that is

$$\mathfrak{m}, \mathfrak{n} \in \operatorname{Smax}(R) \implies \operatorname{height}(\mathfrak{m}) = \operatorname{height}(\mathfrak{n})$$

(iii) A commutative ring $(R, +, \cdot)$ is said to be **catenary** (this word is derived from the Latin word *catena* for *chain*), iff for any two prime ideals $\mathfrak{p}, \mathfrak{q} \in \operatorname{Spec}(R)$ with $\mathfrak{p} \subset \mathfrak{q}$ we have the properties:

(1) The prime ideals $\mathfrak{p}$ and $\mathfrak{q}$ can be connected by a maximal CPI, that is: There is a saturated chain of prime ideals $\mathcal{P} \in \mathrm{CPI}_{\mathfrak{p}}^{\mathfrak{q}}(R)$.

(2) Any two saturated chains of prime ideals $\mathcal{P}, \mathcal{Q} \in \mathrm{CPI}_{\mathfrak{p}}^{\mathfrak{q}}(R)$ have the same length: $\ell(\mathcal{P}) = \ell(\mathcal{Q})$.

(iv) A commutative ring $(R, +, \cdot)$ is said to be **universally catenary**, iff for any commutative R-algebra A we get the implication: If A is finitely generated as an R-algebra, then A also is catenary.

(8.75) Proposition: (viz. 1272)

(i) If $(R, +, \cdot)$ is a holodimensional ring, then it already is equidimensional and catenary and for any prime ideal $\mathfrak{p} \in \operatorname{Spec}(R)$ we have the identity

$$\operatorname{kdim}\left(R \big/ \mathfrak{p}\right) + \operatorname{height}(\mathfrak{p}) \;=\; \operatorname{kdim}(R)$$

(ii) Let $(R, +, \cdot)$ be a commutative ring and $\mathfrak{p} \subseteq \mathfrak{q}$ be nested prime ideals of R, such that $R/\mathfrak{p}$ is holodimensional. Then any saturated chain $\mathcal{P} \in \mathrm{CPI}_{\mathfrak{p}}^{\mathfrak{q}}(R)$, ranging from $\mathfrak{p}$ to $\mathfrak{q}$, is of length

$$\ell(\mathcal{P}) \;=\; \operatorname{kdim}\left(R \big/ \mathfrak{p}\right) - \operatorname{kdim}\left(R \big/ \mathfrak{q}\right) \;=\; \operatorname{height}\left(\mathfrak{q} \big/ \mathfrak{p}\right) \;=\; \operatorname{height}(\mathfrak{q}) - \operatorname{height}(\mathfrak{p})$$

(iii) If $(R,+,\cdot)$ is a holodimensional ring and $\mathfrak{p} \in \operatorname{Spec}(R)$ is any prime ideal of R, then the quotient ring $R/\mathfrak{p}$ also is a holodimensional ring of Krull-dimension

$$\operatorname{kdim}\left(R \Big/ \mathfrak{p}\right) \;=\; \operatorname{kdim}(R) - \operatorname{height}(\mathfrak{p})$$

(iv) If $(R,+,\cdot)$ is a noetherian ring (actually we only need $\operatorname{height}(\mathfrak{p}) < \infty$ for any prime ideal $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$), then the following statements (a) and (b) are equivalent. And in this case R is catenary.

(a) For any prime ideals $\mathfrak{p}, \mathfrak{q} \in \operatorname{Spec}(R)$ such that $\mathfrak{p} \subset_* \mathfrak{q}$ we have $\operatorname{height}(\mathfrak{q}) = \operatorname{height}(\mathfrak{p}) + 1$.

(b) For any prime ideals $\mathfrak{p}, \mathfrak{q} \in \operatorname{Spec}(R)$ such that $\mathfrak{p} \subseteq \mathfrak{q}$ we regard $\mathfrak{q}/\mathfrak{p}$ as a prime ideal in the quotient ring $R/\mathfrak{p}$. And thereby we have the identity

$$\operatorname{height}\left(\mathfrak{q} \Big/ \mathfrak{p}\right) \;=\; \operatorname{height}(\mathfrak{q}) - \operatorname{height}(\mathfrak{p})$$

Nota It might come as a surprise, but the converse is untrue: Even if R is catenary properties (a) and (b) need *not* be true. We will present a counterexample of this in (8.82.(4)).

(v) If $(R,+,\cdot)$ is a holodimensional ring and $\mathfrak{p} \in \operatorname{Spec}(R)$ is any prime ideal of R, then the localisation $R_{\mathfrak{p}}$ also is a holodimensional local ring of Krull-dimension

$$\operatorname{kdim}\big(R_{\mathfrak{p}}\big) \;=\; \operatorname{kdim}(R) - \operatorname{kdim}\left(R \Big/ \mathfrak{p}\right)$$

(vi) If $(R,+,\cdot)$ is an integral domain, that is equidimensional and catenary, then R is holodimensional.

Noetherian Normalisation and Krull Dimension

Let us revisit the noetherian normalisation theorem (8.52) in the light of the notions of Krull's dimension. It will turn out, that finitely generated algebras A over fields are very well-behaved. There are still a lot of powerful theorems for general noetherian rings R, but those of algebras are even better:

(8.76) Proposition: (viz. 1276)

(i) Let $(E,+,\cdot)$ be a field and A a finitely generated E-algebra, such that A also is an integral domain. Then the length of any maximal CPI equals $\operatorname{trdeg}(A:E)$. In particular A is holodimensional and

$$\operatorname{kdim}(A) \;=\; \operatorname{trdeg}(A:E) \;<\; \infty$$

(ii) Let $(E,+,\cdot)$ be a field and $A \neq 0$ be any finitely generated E-algebra. Then A only has finitely many minimal prime ideals and for the the Krull-dimension of A we find the identity

$$\operatorname{kdim}(A) \;=\; \max\left\{ \operatorname{kdim}\left(A \Big/ \mathfrak{n}\right) \;\middle|\; \mathfrak{n} \in \operatorname{Smin}(A) \right\} \;<\; \infty$$

(iii) Any field $(E,+,\cdot)$ is universally catenary, that is any finitely generated E-algebra A is catenary. In fact we even get: For any prime ideal $\mathfrak{p} \trianglelefteq_{\mathfrak{i}} A$, the quotient $A/\mathfrak{p}$ is holodimensional and if $\mathfrak{q} \trianglelefteq_{\mathfrak{i}} A$ is another prime ideal of A, with $\mathfrak{p} \subseteq \mathfrak{q}$, then any saturated CPI $\mathcal{P} \in \mathrm{CPI}_{\mathfrak{p}}^{\mathfrak{q}}(A)$ has the same length

$$\ell(\mathcal{P}) \;=\; \mathrm{kdim}\left(A \Big/ \mathfrak{p}\right) - \mathrm{kdim}\left(A \Big/ \mathfrak{q}\right) \;=\; \mathrm{height}(\mathfrak{q}) - \mathrm{height}(\mathfrak{p})$$

(iv) Let $(E,+,\cdot)$ be a field and $A \neq 0$ be a finitely generated E-algebra. Also consider a chain $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \ldots \subseteq \mathfrak{a}_r \trianglelefteq_{\mathfrak{i}} A$ of proper ideals in A, that is $\mathfrak{a}_r \neq A$, of length $r \in \mathbb{N}$. By (8.52) there are algebraically independent elements $z_1,\ldots,z_n \in A$ and numbers $0 \leq k(1) \leq k(2) \leq \cdots \leq k(r) \leq n$ such that letting $P := E[z_1,\ldots,z_n]$ for any $i \in 1\ldots r$ we have

$$\mathfrak{a}_i \cap P \;=\; z_1P + \cdots + z_{k(i)}P$$

Then (1) A has Krull-dimension n and (2) if A is an integral domain then any of the ideals $\mathfrak{a}_i$ has height $k(i)$. In consequence the numbers n and $k(i)$ are uniquely determined by A resp. the ideals $\mathfrak{a}_i$ independent of the specific normalisation

$$\begin{aligned} \mathrm{kdim}(A) &= n \\ \mathrm{height}(\mathfrak{a}_i) &= k(i) \end{aligned}$$

(8.77) Remark:

(i) If $(E,+,\cdot)$ is a field and $n \in \mathbb{N}$ then the polynomial ring in n variables $E[t_1,\ldots,t_n]$ satisfies the properties required in (8.76.(i)) above. In particular it is an integral domain. And as the variables $\{\, t_1,\ldots,t_n \,\}$ are a transcendence basis of $E[t_1,\ldots,t_n] : E$ we conclude, that $E[t_1,\ldots,t_n]$ is holodimensional of Krull-dimension

$$\mathrm{kdim}\big(E[t_1,\ldots,t_n]\big) \;=\; n$$

(ii) Fix any $k \in 0\ldots n$ then the ideal $\langle t_1,\ldots,t_k\rangle_{\mathfrak{i}}$ of the polynomial ring $E[t_1,\ldots,t_n]$ clearly is a prime ideal of height k. In the next section this property will be formulated, as "$(t_1,\ldots,t_n)$ is a regular sequence of $E[t_1,\ldots,t_n]$".

$$\mathrm{height}\big(\langle t_1,\ldots,t_k\rangle_{\mathfrak{i}}\big) \;=\; k$$

Prob Clearly $E[t_1,\ldots,t_n]/\langle t_1,\ldots,t_k\rangle_{\mathfrak{i}}$ is isomorphic to $E[t_{k+1},\ldots,t_n]$ which is a polynomial ring in $n-k$ variables. And as $E[t_1,\ldots,t_n]$ is holodimensional, we may compute the height of $\langle t_1,\ldots,t_k\rangle_{\mathfrak{i}}$ using (i) above and the formula in (8.75.(i))

$$\mathrm{height}\big(\langle t_1,\ldots,t_k\rangle_{\mathfrak{i}}\big) \;=\; \mathrm{kdim}\big(E[t_1,\ldots,t_n]\big) - \mathrm{kdim}\left(E[t_1,\ldots,t_n] \Big/ \langle t_1,\ldots,t_k\rangle_{\mathfrak{i}}\right) \;=\; k$$

(8.78) Corollary: (viz. 1280)
Let $(E,+,\cdot)$ be a field and $A \neq 0$ a finitely generated, commutative E-algebra Also let $\mathfrak{p} \in \operatorname{Spec}(A)$ be a prime ideal. Then we obtain the following properties

(i) Let $E_\mathfrak{p} := A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ denote the quotient field of the localisation $A_\mathfrak{p}$. This is an E-algebra under the scalar multiplication $a(f/u + \mathfrak{p}A_\mathfrak{p}) := (af)/u\mathfrak{p}A_\mathfrak{p}$. And thereby we get

$$\operatorname{trdeg}\big(E_\mathfrak{p} : E\big) \;=\; \operatorname{kdim}\Big(A \Big/ \mathfrak{p}\Big)$$

(ii) For a CPI $\mathcal{P} = (\mathfrak{p}_0,\ldots,\mathfrak{p}_r)$ of A let us denote $\mathfrak{p} \in \mathcal{P}$ if and only if $\mathfrak{p} = \mathfrak{p}_i$ for some $i \in 0\ldots r$. Then we obtain the following identities

$$\begin{aligned}\operatorname{kdim}\Big(A \Big/ \mathfrak{p}\Big) + \operatorname{height}(\mathfrak{p}) &= \sup\left\{ \ell(\mathcal{P}) \;\middle|\; \begin{array}{l}\mathcal{P} \in \operatorname{CPI}(A)\\ \text{with } \mathfrak{p} \in \mathcal{P}\end{array} \right\}\\ &= \max\left\{ \operatorname{kdim}\Big(A \Big/ \mathfrak{p}_*\Big) \;\middle|\; \begin{array}{l}\mathfrak{p}_* \in \operatorname{Smin}(A)\\ \text{with } \mathfrak{p}_* \subseteq \mathfrak{p}\end{array} \right\}\end{aligned}$$

(iii) By (8.52) there are algebraically independent elements $z_1,\ldots,z_n \in A$ and $k \in 0\ldots n$ such that $A : P$ is finite, where $P := E[z_1,\ldots,z_n]$ and we also get $\mathfrak{p} \cap P = z_1P + \cdots + z_kP$. From this we get a *Noetherian normalisation* of $A/\mathfrak{p}$ in the following way: For any $x \in A$ let us abbreviate the residue element $\overline{x} := x + \mathfrak{p} \in A/\mathfrak{p}$, then we get

(1) $\{\,\overline{z}_{k+1},\ldots,\overline{z}_n\,\} \subseteq A/\mathfrak{p}$ is algebraically independent
(2) $A/\mathfrak{p} : \overline{P}$ is a finite ring-extension, where $\overline{P} := E[\overline{z}_{k+1},\ldots,\overline{z}_n]$
(3) $\operatorname{kdim}(A/\mathfrak{p}) = n - k$
(4) We find an isomorphism of E-algebras, that can be explicitly given to be the following map

$$P \Big/ \mathfrak{p} \cap P \;\xrightarrow{\sim}\; \overline{P} \;:\; f(z_1,\ldots,z_n) + \mathfrak{p} \cap P \mapsto f(0,\ldots,0,\overline{z}_{k+1},\ldots,\overline{z}_n)$$

(5) If $\mathfrak{p} \subseteq \mathfrak{a}_1 \subseteq \ldots \subseteq \mathfrak{a}_r \neq A$ is a chain of proper ideals of A, containing $\mathfrak{p}$ and we are given the ascending chain of numbers $0 \leq k(1) \leq \cdots \leq k(r) \leq n$s, such that $\mathfrak{a}_i \cap P = z_1P + \cdots + z_{k(i)}P$ for any $i \in 1\ldots r$, then we find that $k \leq k(1)$ and

$$\mathfrak{a}_i \Big/ \mathfrak{p} \cap \overline{P} \;=\; \overline{z}_{k+1}\overline{P} + \cdots + \overline{z}_{k(i)}\overline{P}$$

(8.79) Corollary: (viz. 1282)
Let $(E,+,\cdot)$ be a field and A be any E-algebra (not necessarily finitely generated). Let us agree to call the maximal number of algebraically independent elements inside A the *transcendent freedom* of $A : E$

$$\operatorname{tfree}(A : E) \;:=\; \max\{\,\#U \mid U \subseteq A,\, U \text{ algebraically independent}\,\}$$

In particular: If A contains an infinite set $U \subseteq A$ that is algebraically independent, then $\operatorname{tfree}(A) = \infty$. And if $\operatorname{tfree}(A : E) = n$ is finite, then any algebraically independent set $U \subseteq A$ contains no more than n elements. Using this notion we obtain the following statements:

(i) If A is an integral domain, then $\operatorname{tfree}(A : E) = \operatorname{trdeg}(A : E)$.

(ii) If $\mathfrak{q} \in \operatorname{Spec}(A)$ is a prime ideal, then $A/\mathfrak{q}$ becomes an E-algebra under the scalar multiplication $a(x+\mathfrak{q}) := ax + \mathfrak{q}$. And thereby we find the estimate

$$\operatorname{tfree}\left(A \Big/ \mathfrak{q} : E\right) \quad \leq \quad \operatorname{tfree}(A : E)$$

(iii) If A is an integral domain and a finitely generated E-algebra, then we have $\operatorname{kdim}(A) = \operatorname{trdeg}(A : E)$. For a general E-algebra, we still retain the inequality

$$\operatorname{kdim}(A) \quad \leq \quad \operatorname{tfree}(A : E)$$

Nota This inequality may be strict: Consider $F = E(t_1, \ldots, t_n) = \textsc{quot}\big(E[t_1, \ldots, t_n]\big)$ the field of rational functions in n variables. Then $\operatorname{kdim}(F) = 0$, as F is a field. But $\operatorname{trdeg}(F : E) = n$, as the variables $\{ t_1, \ldots, t_n \}$ are algebraically independent.

(iv) If A is a finitely generated E-algebra, that also is an integral domain and $P \leq_{\mathsf{a}} A$ is an E-subalgebra of A, then we get [whether P is finitely generated or not]

$$\operatorname{kdim}(P) \quad \leq \quad \operatorname{kdim}(A)$$

Krull's Theorems

We finally reached the core of dimension theory: Krull's theorems study the connection between the height and the number of generators of an ideal $\mathfrak{a}$ in a noetherian ring R. If we think of an affine variety $X \subseteq E^n$, then $R = E[t_1, \ldots, t_n]$ is the polynomial ring and $\mathfrak{a} = \mathbb{I}(X)$ is the vanishing ideal of X. Then $\operatorname{height}(\mathfrak{a})$ is the dimension of X and $\operatorname{rank}(\mathfrak{a})$ is the minimal number of equations used to define X. It turns out that if we use k equations $f_1, \ldots, f_k \in R$ to define X, then the dimension of X is $n - k$ or more. Without equations we start at n and any additional equation can reduce the dimension by 1, at most. This is the fundamental interpretation behind these theorems:

(8.80) Theorem: (viz. 1283)

(i) *Krull's principal Ideal Theorem:* Let $(R, +, \cdot)$ be a noetherian ring, $a \in R$ an element and let $\mathfrak{p} \in \operatorname{Spec}(R)$ be a prime ideal, that is minimal over $aR \trianglelefteq_{\mathsf{i}} R$. Then $\mathfrak{p}$ has height 1 or less. Formally

$$\mathfrak{p} \in \mathbb{V}(aR)_* \quad \Longrightarrow \quad \operatorname{height}(\mathfrak{p}) \leq 1$$

(ii) *Krull's Height Theorem:* Let $(R, +, \cdot)$ be a noetherian ring and fix $n \in \mathbb{N}$ with $n \geq 1$. If now $\mathfrak{p} \in \operatorname{Spec}(R)$ is a prime ideal, then the following two statements are equivalent

(a) $\operatorname{height}(\mathfrak{p}) \leq n$

(b) There are some $a_1, \ldots, a_n \in \mathfrak{p}$ such that $\mathfrak{p}$ is a minimal prime ideal $\mathfrak{p} \in \mathbb{V}(\mathfrak{a})_*$ over the ideal $\mathfrak{a} := \langle a_1, \ldots, a_n \rangle_{\mathsf{i}}$ generated by these elements.

Nota If $\mathfrak{p} = \mathfrak{a} = \langle a_1, \ldots, a_n \rangle_{\mathsf{i}}$ then $\mathfrak{p}$ is the only minimal prime over $\mathfrak{a}$, in particular $\operatorname{height}(\mathfrak{p}) \leq n$. That means that any (prime) ideal in a noetherian ring has finite height. However there is no upper bound to the number of generators required and hence to the height of prime ideals, such that R may have $\operatorname{kdim}(R) = \infty$, never the less.

(iii) Let $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be a proper ideal $\mathfrak{a} \neq R$ in a noetherian ring $(R,+,\cdot)$. Recall that the rank of $\mathfrak{a}$ as an R-module is $\operatorname{rank}(\mathfrak{a}) = \min\{\, n \in \mathbb{N} \mid \exists\, a_1,\ldots,a_n \in R : \mathfrak{a} = \langle a_1,\ldots,a_n\rangle_{\mathrm{i}} \,\}$ the minimal number of generators of $\mathfrak{a}$. And it always takes at least n elements, to build up an ideal of height n

$$\operatorname{height}(\mathfrak{a}) \;\leq\; \operatorname{rank}(\mathfrak{a})$$

(iv) If $(R,+,\cdot)$ is a noetherian ring and $(\mathfrak{p}_0,\ldots,\mathfrak{p}_r)$ is a CPI of R where $r \geq 1$ and $a \in \mathfrak{p}_r$ is any element, then there is another CPI of R, of the form $(\mathfrak{p}_0,\widetilde{\mathfrak{p}}_1,\ldots,\widetilde{\mathfrak{p}}_{r-1},\mathfrak{p}_r)$, such that we get $a \in \widetilde{\mathfrak{p}}_1$.

(v) Let $(R,+,\cdot)$ be a noetherian ring, $\mathfrak{a}$, $\mathfrak{b} \trianglelefteq_{\mathrm{i}} R$ be ideals of R, such that $\mathfrak{a} \subseteq \mathfrak{b}$ and fix m, $n \in \mathbb{N}$ such that $0 \leq m \leq n$. Also consider $a_1,\ldots,a_m \in R$ such that $\mathfrak{a} = \langle a_1,\ldots,a_m\rangle_{\mathrm{i}}$ and suppose $\operatorname{height}(\mathfrak{a}) = m$ and $\operatorname{height}(\mathfrak{b}) \geq n$. Then we can append elements $a_{m+1},\ldots,a_n \in \mathfrak{b}$ with the following property: Let us denote $\mathfrak{a}_k := \langle a_1,\ldots,a_k\rangle_{\mathrm{i}}$, in particular $\mathfrak{a}_m = \mathfrak{a}$. Then for any $k \in m\ldots n$ we get $\operatorname{height}(\mathfrak{a}_k) = k$. In fact we even get a much stronger property: If $\mathfrak{p}_k \in \operatorname{Spec}(R)$ is any prime ideal, minimal over $\mathfrak{a}_k$ then we have

$$\operatorname{height}(\mathfrak{p}_k) \;=\; k$$

(vi) Let $(\mathfrak{p}_0,\ldots,\mathfrak{p}_r)$ be a CPI in a noetherian ring $(R,+,\cdot)$ such that $r = \operatorname{height}(\mathfrak{p}_r)$. Then there are some elements $a_1,\ldots,a_r \in R$ such that for any $k \in 0\ldots r$ the ideal $\mathfrak{a}_k := \langle a_1,\ldots,a_k\rangle_{\mathrm{i}}$ has the following two properties

(1) $\operatorname{height}(\mathfrak{a}_k) = k$

(2) $\mathfrak{p}_k$ is minimal over $\mathfrak{a}_k$

(vii) Let $(R,+,\cdot)$ is a noetherian ring and $a \in \operatorname{NZD}(R)$ be a non-zero-divisor that is contained in $a \in \mathfrak{p} \in \operatorname{Spec}(R)$. Then $\mathfrak{p}/aR$ is a prime ideal in the quotient ring R/aR and the height of this ideal is one less, than the height of $\mathfrak{p}$. Formally that is

$$\operatorname{height}\left(\mathfrak{p} \Big/ {}_{aR}\right) \;=\; \operatorname{height}(\mathfrak{p}) - 1$$

(8.81) Remark:
Let us analyse what $\operatorname{height}(\mathfrak{p}) = n$ means for a prime ideal $\mathfrak{p} \in \operatorname{Spec}(R)$ in a noetherian ring R. Due to the equivalence in Krull's height theorem we can break it down into the following two properties

(1) There are some $a_1,\ldots,a_n \in \mathfrak{p}$ such that $\mathfrak{p}$ is a minimal prime ideal $\mathfrak{p} \in \mathbb{V}(\mathfrak{a})_*$ over the ideal $\mathfrak{a} := \langle a_1,\ldots,a_n\rangle_{\mathrm{i}}$ generated by these elements.

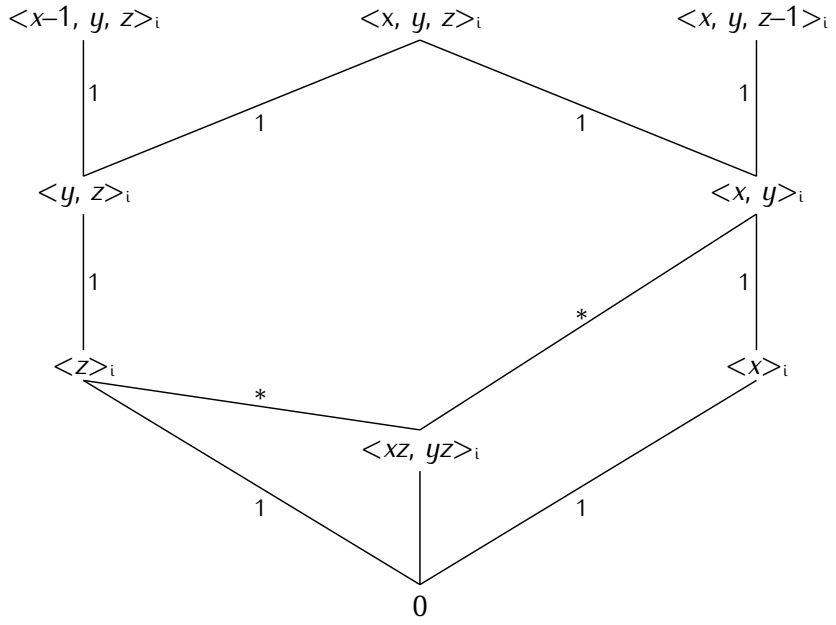
(2) For any $b_1,\ldots,b_m \in \mathfrak{p}$ with $0 \leq m < n$ there is another prime ideal $\mathfrak{p}' \in \operatorname{Spec}(R)$ such that $\mathfrak{b} \subseteq \mathfrak{p}' \subset \mathfrak{p}$, where $\mathfrak{b} := \langle b_1,\ldots,b_m\rangle_{\mathrm{i}}$ denotes the ideal generated by these elements.

This is readily apparent, as (2) is just the negation of (b) in (8.80.(ii)). The converse is also true: If $\mathfrak{p} \in \operatorname{Spec}(R)$ satisfies (1) and (2), then $\operatorname{height}(\mathfrak{p}) = n$. In fact we have to check (2) for $m = n-1$ only, as this property then is inherited by all $0 \leq m < n$.

(8.82) Example: (viz. 1288)
If A is not an integral domain, weird things may happen: Consider the polynomial ring in 3 variables over a field $R = E[x,y,z]$. Then we take a look at the E-algebra

$$A \;:=\; E[x,y,z] \Big/ \mathfrak{a} \quad \text{where} \quad \mathfrak{a} \;:=\; \langle xz, yz \rangle_{\mathrm{i}}$$

Geometrically speaking A is corresponds to the union of the xy-plane $\langle z \rangle_{\mathrm{i}}$ and the z-axis $\langle x,y \rangle_{\mathrm{i}}$. The following diagram illustrates the structure some ideals in R. The numbers stand for the difference in height and the asterisks indicate that the upper ideal is minimal over the lower one. For any polynomial $f \in E[x,y,z]$ let us abbreviate $\overline{f} := f + \mathfrak{a} \in A$, then A has the following properties



(1) Both zR and $xR + yR$ are prime ideals, that are minimal over $\mathfrak{a}$. That means, that an ideal $\mathfrak{a}$ may have minimal primes of different height on top of it.

(2) $\overline{z}A \subset \overline{y}A + \overline{z}A \subset \overline{x}A + \overline{y}A + \overline{z}A$ is a chain of prime ideals of A and hence $\operatorname{kdim}(A) = 2$. This shows, that not every element contained in $\mathfrak{a}$ reduces the dimension of A, by 1.

(3) The set $\{\, \overline{x}, \overline{y} \,\} \subseteq A$ is something like a transcendence basis: It is algebraically independent and $A : P$ is an algebraic extension, for $P := E[\overline{x}, \overline{y}]$. However $A : P$ is not a finite extension and as A is not an integral domain algebraic dependence is not a dependence relation.

(4) As E is a field and A is an E-algebra generated by finitely many elements $\{\, \overline{x}, \overline{y}, \overline{z} \,\}$, A is catenary by (8.76.(iii)). However the ideals $\overline{\mathfrak{m}} := \langle x,y,z \rangle_{\mathrm{i}} / \mathfrak{a}$ and $\overline{\mathfrak{q}} = \langle x,y \rangle_{\mathrm{i}} / \mathfrak{a}$ satisfy

$$\operatorname{height}\left(\overline{\mathfrak{m}} \Big/ \overline{\mathfrak{q}} \right) \;=\; 1 \;<\; 2 - 0 \;=\; \operatorname{height}(\overline{\mathfrak{m}}) - \operatorname{height}(\overline{\mathfrak{q}})$$

(8.83) Example: (viz. 1289)
It can happen, that the height of a prime ideal is strictly less, than the minimal number of generators of a prime ideal: Consider any field E and regard polynomial ring in three resp. in one variable: $E[x,y,z]$ and $E[t]$. Then we regard the following homomorphism of E-algebras

$$\pi \;:\; E[x,y,z] \;\to\; E[t] \;:\; f \mapsto f(t^3,t^4,t^5)$$

(1) Then $\mathfrak{p} := \mathrm{kn}(\pi)$ is a prime ideal, strictly contained in $\mathfrak{m} = \langle x,y,z\rangle_{\mathrm{i}}$ and therefore $\mathrm{height}(\mathfrak{p}) = 2$.

(2) Also $\mathfrak{p} = \langle f_1,f_2,f_3\rangle_{\mathrm{i}}$ is generated by 3 elements, namely $f_1 = xz - y^2$, $f_2 = yz - x^3$ and $f_3 = x^2y - z^2$. Yet $\mathfrak{p}$ *cannot* be generated by 2 (or fewer) elements.

(8.84) Proposition: (viz. 1293)
Let $(R,+,\cdot)$ be a notherian ring and $\mathfrak{p} \subset \mathfrak{q}$ be two nested prime ideals of R. Then there are either no or infinitely many prime ideals $\mathfrak{p}'$ in between. That is the following set either is empty or infinite

$$\#\left\{\, \mathfrak{p}' \in \mathrm{Spec}(R) \mid \mathfrak{p} \subset \mathfrak{p}' \subset \mathfrak{q} \,\right\} \;\in\; \{\,0,\infty\,\}$$

And thereby a noetherian ring with only finitely many prime ideals either is a field or one-dimensional

$$\#\mathrm{Spec}(R) < \infty \quad\Longrightarrow\quad \mathrm{kdim}(R) \leq 1$$

(8.85) Theorem: (viz. 1291)

(i) Let $(R,+,\cdot)$ be a commutative ring and $\mathfrak{u} \in R[t]$ be a prime ideal in the polynomial ring over R. Let $\mathfrak{p} := \mathfrak{u} \cap R$, which is a prime ideal in R. Then the following two statements are equivalent

 (a) $\mathfrak{u} = \mathfrak{p}[t]$

 (b) There is a prime ideal $\mathfrak{v} \in R[t]$ that also lies over $\mathfrak{p}$ in R but lies strictly over $\mathfrak{u}$ in $R[t]$. That is $\mathfrak{v}$ satisfies the properties: $\mathfrak{u} \subset \mathfrak{v}$ and $\mathfrak{u} \cap R = \mathfrak{v} \cap R$.

(ii) Let $(R,+,\cdot)$ be a commutative ring, $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be any ideal and $\mathfrak{p} \in \mathrm{Spec}(R)$ be a prime ideal, such that $\mathfrak{a} \subseteq \mathfrak{p}$. Then we find the equivalence of the following two statements

 (a) $\mathfrak{p}$ is a minimal prime ideal over $\mathfrak{a}$

 (b) $\mathfrak{p}[t]$ is a minimal prime ideal over $\mathfrak{a}[t]$

(iii) Let $(R,+,\cdot)$ be a noetherian ring and $\mathfrak{p} \in \mathrm{Spec}(R)$ be a prime ideal. Then the height of $\mathfrak{p}$ in R equals the height of $\mathfrak{p}[t]$ in $R[t]$, formally that is

$$\mathrm{height}\big(\mathfrak{p}\big) \;=\; \mathrm{height}\big(\mathfrak{p}[t]\big)$$

(iv) If $(R,+,\cdot)$ is any commutative ring of Krull-dimension $n := \mathrm{kdim}(R)$. Then the Krull-dimension of the polynomial ring $R[t]$ has the following bounds

$$n+1 \;\leq\; \mathrm{kdim}\big(R[t]\big) \;\leq\; 2n+1$$

Nota these are not only theoretical bounds: In fact it can be proved, that any value in between is assumed by some ring. (■) Refer to P. Jaffard *Théorie de la dimension dans les anneaux des polynomes*. Memorial Sci. Math. 146 (1960).

(v) If $(R, +, \cdot)$ is a noetherian ring and $n \in \mathbb{N}$, then the Krull-dimension of the polynomial ring in n variables over R is given to be

$$\operatorname{kdim}\big(R[t_1, \ldots, t_n]\big) \;=\; \operatorname{kdim}(R) + n$$

8.8 Spectrum of a Ring

We have come a long way and have seen, that prime ideals are an extremely helpful tool, all around in algebra. They can be thought of as the proper generalisation of prime numbers in the integers and prime (mostly called irreducible) polynomials in $E[t]$. The common ground is, that they can be used to decompose more complex structures into parts, that are easier to control. For example recall the Lasker-Noether theorem (2.101), which is a generalisation of prime decomposition or Noetherian filtrations (5.14) that provide a way of dealing with a module, one step at a time.
But this is not the end of the story. Prime ideals are a strange looking glass through which we can study the structure af a ring. For example prime avoidance (2.14.(iii)) is a consequence of the prime property. And if F is an algebraically closed field, then $\mathrm{Smax}(F[t]) = \{\, (t-x)F[t] \mid x \in F \,\}$ - that is F itself corresponds to a special subset of the prime spectrum of $F[t]$. For a general field, the maximal spectrum of $F[t]$ will have additional points, that do not correspond to elements of F.
It is tempting to study the structure of the spectrum of a ring in order to learn something about the ring itself. This allows to introduce topology to the problem, but it also takes some time to get accustomed to the strange, distorted images, this looking glass provides.

Let us recollect, what we know so far: In (2.16) we have introduced the concept of the set of all prime ideals containing another ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$, for a commutative ring $(R,+,\cdot)$. This concept has a twin sister: The intersection of a set pf prime ideals, which is another ideal of R

$$\begin{aligned}
\mathbb{V} \;:\; \mathrm{Ideal}(R) \;&\to\; \mathcal{P}\big(\mathrm{Spec}(R)\big) \;:\; \mathfrak{a} \;\mapsto\; \{\, \mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{a} \subseteq \mathfrak{p} \,\} \\
\mathbb{I} \;:\; \mathcal{P}\big(\mathrm{Spec}(R)\big) \;&\to\; \mathrm{Ideal}(R) \;:\; \mathcal{P} \;\mapsto\; \begin{cases} \bigcap \mathcal{P} \text{ if } \mathcal{P} \neq \emptyset \\ R \text{ if } \mathcal{P} = \emptyset \end{cases}
\end{aligned}$$

It is clear, that $\mathbb{V}(0) = \mathrm{Spec}(R)$ and $\mathbb{V}(R) = \emptyset$. Also we have seen in (2.16) that for a finite resp. arbitrary collection of ideals $\mathfrak{a}_i \trianglelefteq_{\mathrm{i}} R$ the map $\mathbb{V}$ has the following properties

$$\begin{aligned}
\mathbb{V}\left(\sum_{i\in I} \mathfrak{a}_i\right) &= \bigcap_{i\in I} \mathbb{V}(\mathfrak{a}_i) \\
\mathbb{V}\left(\bigcap_{i=1}^{n} \mathfrak{a}_i\right) &= \bigcup_{i=1}^{n} \mathbb{V}(\mathfrak{a}_i)
\end{aligned}$$

This is the reason why we get a topology on $\mathrm{Spec}(R)$ by taking sets of the form $\mathbb{V}(\mathfrak{a})$ to be the closed sets of the topology - this is guaranteed in the easy proposition (6.12.(ii)). It is this topology that we introduce in the next definition. Also it is clear, that for any ideals $\mathfrak{a}$, $\mathfrak{b}$ of R, respectively subsets $\mathcal{P}$, $\mathcal{Q} \subseteq \mathrm{Spec}(R)$ the maps $\mathbb{V}$ and $\mathbb{I}$ are order-reversing, that is $\mathfrak{a} \subseteq \mathfrak{b}$ turns into $\mathbb{V}(\mathfrak{b}) \subseteq \mathbb{V}(\mathfrak{a})$ and likewise $\mathcal{P} \subseteq \mathcal{Q}$ turns into $\mathbb{I}(\mathcal{Q}) \subseteq \mathbb{I}(\mathcal{P})$. Also any proper ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ satisfies

$$\mathfrak{a} \;\subseteq\; \sqrt{\mathfrak{a}} \;=\; \bigcap \{\, \mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{a} \subseteq \mathfrak{p} \,\} \;=\; \mathbb{I}\big(\mathbb{V}(\mathfrak{a})\big)$$

according to (2.25.(i)) and $\mathbb{I}(\mathcal{P}) \subseteq \mathfrak{p}$ for any $\mathfrak{p} \in \mathcal{P} \subseteq \operatorname{Spec}(R)$ is trivial, such that $\mathcal{P} \subseteq \mathbb{V}(\mathbb{I}(\mathcal{P}))$ is true, as well. Then (0.22) tells us, that $(\mathbb{V}, \mathbb{I})$ forms contra-variant *Galois connection*. That is $\mathbb{V}\mathbb{I}\mathbb{V} = \mathbb{V}$ and $\mathbb{I}\mathbb{V}\mathbb{I} = \mathbb{I}$ and we obtain a 1-to-1 correspondence

$$\begin{array}{rcl} \operatorname{Srad}(R) & \longleftrightarrow & \mathcal{Z}(R) \\ \mathfrak{a} & \mapsto & \mathbb{V}(\mathfrak{a}) \\ \mathbb{I}(\mathcal{P}) & \hookleftarrow & \mathcal{P} \end{array}$$

Thereby $\mathcal{Z}(R) := \{\, \mathbb{V}(\mathfrak{a}) \mid \mathfrak{a} \trianglelefteq_{\mathrm{i}} R \,\}$ is the collection of closed subsets of $\operatorname{Spec}(R)$ just by definition and the image of $\mathbb{I}$ equals $\operatorname{Srad}(R) = \{\, \mathbb{I}(\mathcal{P}) \mid \mathcal{P} \subseteq \operatorname{Spec}(R) \,\}$, as can be seen in the following way:

Prob If $\mathfrak{a} \in \operatorname{Srad}(R)$ is a radical ideal of R, then either $\mathfrak{a} = R = \mathbb{I}(\emptyset)$ or $\mathfrak{a} \neq R$ is proper. In the latter case we have $\mathbb{I}(\mathbb{V}(\mathfrak{a})) = \sqrt{\mathfrak{a}} = \mathfrak{a}$ by (2.25.(i)), such that $\mathfrak{a}$ is contained in the image of $\mathbb{I}$, again. If conversely $\mathfrak{a} = \mathbb{I}(\mathcal{P})$, for some $\mathcal{P} \neq \emptyset$, then $\mathbb{I}(\mathcal{P})$ is a radical ideal, due to (2.22.(v)).

(8.86) Definition:
Let $(R, +, \cdot)$ be any commutative ring and $\operatorname{Spec}(R) := \{\, \mathfrak{p} \trianglelefteq_{\mathrm{i}} R \mid \mathfrak{p} \text{ is a prime ideal} \,\}$ be the collection of all prime ideals of R. Then we introduce the **Zariski topology** on $\operatorname{Spec}(R)$ in the following way: A subset $U \subseteq \operatorname{Spec}(R)$ is said to be *open*, iff

$$U \subseteq \operatorname{Spec}(R) \text{ open} \quad :\Longleftrightarrow \quad \exists\, \mathfrak{a} \trianglelefteq_{\mathrm{i}} R \,:\, U = \operatorname{Spec}(R) \setminus \mathbb{V}(\mathfrak{a})$$

The collection of closed sets of $\operatorname{Spec}(R)$ is denoted by $\mathcal{Z}(R) := \{\, \mathbb{V}(\mathfrak{a}) \mid \mathfrak{a} \trianglelefteq_{\mathrm{i}} R \,\}$ and the collection of open sets of $\operatorname{Spec}(R)$ is denoted by $\mathcal{T}(R) := \{\, \operatorname{Spec}(R) \setminus \mathbb{V}(\mathfrak{a}) \mid \mathfrak{a} \trianglelefteq_{\mathrm{i}} R \,\}$. Is R is understood, we will sometimes write $\mathcal{Z}$ or $\mathcal{T}$ for these sets, only. The topological space $(\operatorname{Spec}(R), \mathcal{T}(R))$ is said to be the (base space of the) **affine scheme** of R.

(8.87) Remark:
Let $(R, +, \cdot)$ be a commutative ring and $X := \operatorname{Spec}(R)$ its prime spectrum. Then we regard X in the Zariski topology $\mathcal{T}$ introduced above. If now $\mathfrak{p} \in X$ is point in X (i.e. any prime ideal of R), then the open neighbourhood filter of $\mathfrak{p}$ is given to be

$$\mathcal{T}(\mathfrak{p}) \;=\; \{\, X \setminus \mathbb{V}(\mathfrak{a}) \mid \mathfrak{a} \trianglelefteq_{\mathrm{i}} R,\, \mathfrak{a} \setminus \mathfrak{p} \neq \emptyset \,\}$$

More generally for any subset $P \subseteq X$ we find that the set of open neighbourhoods of P is given to be

$$\mathcal{T}(P) \;=\; \{\, X \setminus \mathbb{V}(\mathfrak{a}) \mid \mathfrak{a} \trianglelefteq_{\mathrm{i}} R,\, P \cap \mathbb{V}(\mathfrak{a}) = \emptyset \,\}$$

Prob by definition any open set $U \subseteq X$ is of the form $U = X \setminus \mathbb{V}(\mathfrak{a})$ for some ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$. Therefore $\mathfrak{p} \in U$ is equivalent, to $\mathfrak{p} \notin \mathbb{V}(\mathfrak{a})$. That is *non* $\mathfrak{a} \subseteq \mathfrak{p}$. Again this can be put as: There is some $a \in \mathfrak{a}$ with $a \notin \mathfrak{p}$, which turns into $\mathfrak{a} \setminus \mathfrak{p} \neq \emptyset$. Now for $P \subseteq X$, again $U \in \mathcal{T}(P)$ is of the form $U = X \setminus \mathbb{V}(\mathfrak{a})$. Hereby $P \subseteq X \setminus \mathbb{V}(\mathfrak{a})$ is equivalent to $P \cap \mathbb{V}(\mathfrak{a}) = \emptyset$.

The fact that $\mathcal{Z}(R)$ forms the closed set of a topology on $\mathrm{Spec}(R)$ already contains several algebraic properties of ideals. Let us take a first glance how other basic algebraic properties translate into topological properties of the spectrum:

(8.88) Proposition: (viz. 1306)
Let $(R, +, \cdot)$ be a commutative ring and $X := \mathrm{Spec}(R)$ be its prime spectrum endowed with the Zariski topology. Then we obtain the following statements

(i) For any subset $P \subseteq X$ the closure of P is given to be $\overline{P} = \mathbb{V}(\mathbb{I}(P))$.

(ii) The closed points of X are precisely the maximal ideals of R. That is for any prime ideal $\mathfrak{p} \in X$ we obtain the following equivalence

$$\{\,\mathfrak{p}\,\} \subseteq X \text{ closed} \quad \Longleftrightarrow \quad \mathfrak{p} \in \mathrm{Smax}(R)$$

(iii) For any $a \in R$ let us denote the set $B(a) := \{\,\mathfrak{p} \in X \mid a \notin \mathfrak{p}\,\}$. Such a set is called a *principal open set*, due to: (1) $B(a) = X \setminus \mathbb{V}(aR) \subseteq X$ is an open set and (2) for any $a, b \in R$ we have $B(a) \cap B(b) = B(ab)$. And thereby (3) the set $\mathcal{B} := \{\,B(a) \mid a \in R\,\}$ is a base of the Zariski-topology on X. In fact if $U = X \setminus \mathbb{V}(\mathfrak{a})$ is an open set, then we have the identity

$$U \;=\; \bigcup_{a \in \mathfrak{a}} B(a)$$

(iv) The prime spectrum of a commutative ring is a T_0-space (aka *Kolmogorov*-space): That is for any two points $\mathfrak{p}, \mathfrak{q} \in X$ with $\mathfrak{p} \neq \mathfrak{q}$ there is some open set $U \subseteq X$ such that

$$\big(\mathfrak{p} \in U \text{ and } \mathfrak{q} \notin U\big) \;\text{ or }\; \big(\mathfrak{p} \notin U \text{ and } \mathfrak{q} \in U\big)$$

(v) The prime spectrum of a commutative ring, is compact space. That is for any collection $U_i \subseteq X$ of open subsets (where $i \in I$ for some $I \neq \emptyset$) we get the implication

$$X = \bigcup_{i \in I} U_i \quad \Longrightarrow \quad \exists\, \Omega \subseteq I \text{ finite, such that } X = \bigcup_{i \in \Omega} U_i$$

(vi) If $(S, +, \cdot)$ is another commutative ring and $\varphi : R \to S$ is a homomorphism of rings then we get a continuous map (called the **comorphism**) of φ on the spectra of R and S, by virtue of

$$\varphi^* \;:\; \mathrm{Spec}(S) \to \mathrm{Spec}(R) \;:\; \mathfrak{u} \mapsto \varphi^{-1}(\mathfrak{u})$$

(vii) If $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ then the comorphism of $\varrho : R \twoheadrightarrow R/\mathfrak{a} : x \mapsto x + \mathfrak{a}$ is a closed embedding with image $\mathbb{V}(\mathfrak{a})$ [that is ϱ^* is injective, continuous and closed and thereby a homeomorphism onto $\mathbb{V}(\mathfrak{a})$]

$$\varrho^* \;:\; \mathrm{Spec}\left(R \big/ \mathfrak{a}\right) \hookrightarrow \mathrm{Spec}(R) \;:\; \mathfrak{p} \big/ \mathfrak{a} \mapsto \mathfrak{p}$$

(viii) If $U \subseteq R$ is a multiplicatively closed set, then the comorphism of $\kappa : R \to U^{-1}R : a \mapsto a/1$ is a homeomorphism onto the subset $\{\, \mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \cap U = \emptyset \,\}$ of the spectrum of R

$$\kappa^* \;:\; \operatorname{Spec}\big(U^{-1}R\big) \;\hookrightarrow\; \operatorname{Spec}(R) \;:\; U^{-1}\mathfrak{p} \mapsto \mathfrak{p}$$

(8.89) Lemma: (viz. 1308)
Let $(R, +, \cdot)$ be a commutative ring, u, $v \in R$ and $X := \operatorname{Spec}(R)$. Recall the principal open sets $B(u) := \{\, \mathfrak{p} \in X \mid u \notin \mathfrak{p} \,\}$. Suppose we have $B(v) \subseteq B(u)$, then we get the following statements:

(i) There are some $n \in \mathbb{N}$ and $p \in R$ such that $v^n = pu$. And thereby $u/1 \in R_v$ is invertible, with inverse $(u/1)^{-1} = p/v^n$.

(ii) We obtain a homomorphism ϱ_u^v of rings (called the *canonical restriction*) from R_u to R_v by the definition below. And in truth this homomorphism is independent of the specific choice of n and p.

$$\varrho_u^v \;:\; R_u \;\to\; R_v \;:\; \frac{a}{u^m} \;\mapsto\; \frac{ap^m}{v^{mn}} \;=\; \frac{a}{1} \cdot \Big(\frac{u}{1}\Big)^{-m}$$

(iii) If even $B(u) = B(v)$, then the canonical restriction ϱ_u^v is an isomorphism of rings, with inverse homomorphism $(\varrho_u^v)^{-1} = \varrho_v^u$. And if u, v and $w \in R$, such that $B(w) \subseteq B(v) \subseteq B(u)$, then the canonical restrictions satisfy the composition property $\varrho_v^w \, \varepsilon_u^v = \varrho_u^w$.

Irreducible Components
The above proposition is a neat example of how the algebraic properties (e.g. being a homomorphism of rings) translates into topological properties (e.g. being a continuous map). One of the most important notions in algebra are prime ideals. In the following we will study the topological counterpart: irreducible sets. Minimal prime ideals of R will correspond to *irreducible components* of $X = \operatorname{Spec}(R)$, that are a refinement of the connected components of X.

(8.90) Definition: (viz. 1309)
Let $(X, \mathcal{T})$ be a topological space and $I \subseteq X$ be a subset. As always we regard I in the relative topology $\mathcal{T} \cap I$. Then I is said to be **irreducible**, iff it satisfies one of the following equivalent conditions

(a) I cannot be written as a union of two closed, proper subsets, that is: If C and $D \subseteq I$ are closed subsets, such that $I = C \cup D$, then we already have $I = C$ or $I = D$.

(b) I cannot be written as a union of finitely many closed, proper subsets, that is: Given $n \geq 1$ subsets $C_1, \ldots, C_n \subseteq I$ such that any $C_i \subseteq I$ is closed (in the relative topology), we get the implication

$$I = \bigcup_{i=1}^{n} C_i \quad \Longrightarrow \quad \exists\, k \in 1 \ldots n : I = C_k$$

(c) If I is covered by finitely closed sets then I is already contained in one of those sets, that is: Given finitely many closed subsets $C_1, \ldots, C_n \subseteq X$, we get the implication

$$I \subseteq \bigcup_{i=1}^{n} C_i \quad \Longrightarrow \quad \exists\, k \in 1 \ldots n : I \subseteq C_k$$

(d) Every two non-empty, open subsets of I have non-empty intersection, that is: If $U, V \subseteq I$ are open subsets, such that $U \neq \emptyset$ and $V \neq \emptyset$, then we also get $U \cap V \neq \emptyset$.

(e) Every non-empty, open subset of I already is dense in I (i.e. its closure in I is I). More formally: For any open subset $U \subseteq I$ with $U \neq \emptyset$ we get $\overline{U} \cap I = I$.

For the moment being let us denote $\mathcal{I} := \{ I \subseteq X \mid \text{(a)} \}$ the family of all irreducible subsets of X. Then we introduce the set of **irreducible components** of X to be the maximal irreducible subsets of X

$$\operatorname{IRR}(X) \;:=\; \mathcal{I}^* \;=\; \{ I \in \mathcal{I} \mid I \subseteq J \in \mathcal{I} \implies I = J \}$$

It is evident, that the closure $I_x := \overline{\{ x \}}$ of any point $x \in X$ of X is irreducible and we call $x \in X$ the **generic point** of I_x. If X is a T_0-space, then the generic point of a set even is unique, i.e. we then get

$$X \text{ is } T_0,\ \overline{\{ x \}} = \overline{\{ y \}} \quad\implies\quad x = y$$

Nota Not every irreducible set has a generic point: E.g. consider an infinite set X in the *cofinite topology*. That is the open sets $U \subseteq X$ are $U = \emptyset$ and those U, such that $X \setminus U$ is finite. Then any $\{ x \}$ is closed and thereby X cannot have a generic point. But as X is infinite, it is irreducible - the only closed sets apart from X are finite.

(8.91) Proposition: (viz. 1310)
Let $(X, \mathcal{T}_X)$ and $(Y, \mathcal{T}_Y)$ be any two topological spaces, then we obtain the following statements concerning irreducible sets

(i) For an arbitrary subset $I \subseteq X$ the following statements are equivalent

 (a) I is irreducible

 (b) the closure $\overline{I}$ of I is irreducible

 (c) every open subset $P \subseteq I$ of I is irreducible

(ii) Every irreducible set is contained in an irreducible component. That is for any irreducible subset $I \subseteq X$ there is some $J \in \operatorname{IRR}(X)$ such that $I \subseteq J$.

(iii) If $I \subseteq X$ is irreducible, then I is connected, in the sense of (6.34).

(iv) The image of an irreducible set under a continuous map is irreducible, again. That is if $f : X \to Y$ is continuous and $I \subseteq X$ is irreducible, then the image $f(I) \subseteq Y$ is irreducible, too.

(v) If X is a non-empty *Hausdorff space* (that is $X \neq \emptyset$ and for any two $x, y \in X$ with $x \neq y$ there are open subsets $U, V \subseteq X$ such that $x \in U$, $y \in V$ and $U \cap V = \emptyset$), then the irreducible components of X are precisely the sets containing a single point, formally

$$\operatorname{IRR}(X) \;=\; \{ \{ x \} \mid x \in X \}$$

(8.92) Proposition: (viz. 1312)

(i) Let $(R,+,\cdot)$ be an integral domain, then $\mathrm{Spec}(R)$ is an irreducible topological space (in the Zariski topology) and the zero-ideal $0 \trianglelefteq_{\mathfrak{i}} R$ is the generic point of $\mathrm{Spec}(R)$.

(ii) If $(R,+,\cdot)$ is a reduced commutative ring (i.e. $\mathrm{NIL}(R) = 0$) such that $\mathrm{Spec}(R)$ is irreducible (in the Zariski topology), then R already is an integral domain.

(iii) We can generalize (i): If $(R,+,\cdot)$ is any commutative ring and $\mathfrak{p} \trianglelefteq_{\mathfrak{i}} R$ is a prime ideal, then $\mathbb{V}(\mathfrak{p}) \subseteq \mathrm{Spec}(R)$ is an irreducible set (in the Zariski topology) and $\mathfrak{p}$ is its generic point. And thereby we find the equivalence of the following two statements, for any subset $I \subseteq \mathrm{Spec}(R)$:

 (a) $I = \mathbb{V}(\mathfrak{p})$ for some prime ideal $\mathfrak{p} \trianglelefteq_{\mathfrak{i}} R$

 (b) I is a non-empty, closed irreducible subset of $\mathrm{Spec}(R)$

(iv) Let $(R,+,\cdot)$ be a commutative ring and abbreviate its prime spectrum by $X := \mathrm{Spec}(R)$ (in the Zariski topology). Then the irreducible components of R are precisely the sets $\mathbb{V}(\mathfrak{p})$, where $\mathfrak{p}$ is a minimal prime ideal of R. Formally that is the identity, of

$$\mathrm{IRR}(X) \;=\; \{\, \mathbb{V}(\mathfrak{p}) \;\mid\; \mathfrak{p} \in \mathrm{Smin}(R) \,\}$$

(8.93) Proposition: (viz. 1311)
Let $(X,\mathcal{T})$ be a non-empty topological space, then the irreducible components of X satisfy the properties

- $X = \bigcup \mathrm{IRR}(X)$
- $\forall\, I \in \mathrm{IRR}(X)$ we get $I \neq \emptyset$ is non-empty
- $\forall\, I \in \mathrm{IRR}(X)$ we get $I \subseteq X$ is closed and irreducible
- $\forall\, I \subseteq X$ irreducible $\exists\, J \in \mathrm{IRR}(X)$ with $I \subseteq J$

And for any finite family of subsets $\mathcal{I}$ of X (i.e. $\mathcal{I} \subseteq \mathcal{P}(X)$ and $\#\mathcal{I} < \infty$) we have $\mathcal{I} = \mathrm{IRR}(X)$ if and only if $\mathcal{I}$ satisfies all of the following three properties

(1) $X = \bigcup \mathcal{I}$

(2) $\forall\, I \in \mathcal{I}$ we get $I \subseteq X$ is closed and irreducible

(3) $\forall\, I \in \mathcal{I}$ we get $X \neq \bigcup \{\, J \in \mathcal{I} \mid I \neq J \,\}$

(8.94) Proposition: (viz. 1313)
Let $(X,\mathcal{T})$ be a topological space and fix an open subset $U \subseteq X$ (inheriting the relative topology). Then let us denote the closed, irreducible subsets of X and U respectively by

$$\begin{aligned} \mathcal{I}(X) &:= \{\, J \subseteq X \mid J \text{ closed and irreducible} \,\} \\ \mathcal{I}(U) &:= \{\, I \subseteq U \mid I \text{ closed and irreducible} \,\} \end{aligned}$$

Then we obtain a one-to-one correspondence between the non-empty sets of $\mathcal{I}(U)$ and the sets of $\mathcal{I}(X)$ with non-empty $J \cap U$, given by (where the closure $\overline{I}$ is taken in X)

$$\begin{array}{rcl} \{\, I \in \mathcal{I}(U) \mid I \neq \emptyset \,\} & \longleftrightarrow & \{\, J \in \mathcal{I}(X) \mid J \cap U \neq \emptyset \,\} \\ I & \mapsto & \overline{I} \\ J \cap U & \hookleftarrow & J \end{array}$$

This correspondence even correlates the irreducible components of U to the irreducible components of X with non-empty intersection $J \cap U$

$$\begin{array}{rcl} \operatorname{IRR}(U) & \longleftrightarrow & \{\, J \in \operatorname{IRR}(X) \mid J \cap U \neq \emptyset \,\} \\ I & \mapsto & \overline{I} \\ J \cap U & \hookleftarrow & J \end{array}$$

And this correspondence also preserves generic points - let $J \in \mathcal{I}(X)$ such that $J \cap U \neq \emptyset$ and consider any $x \in X$. Then we get the equivalence (where the closure of $\{\, x \,\}$ on the left-hand side is to be taken in U and the closure on the right-hand side is taken in X)

$$J \cap U = \overline{\{\, x \,\}} \iff J = \overline{\{\, x \,\}}$$

Topological Dimension

In the previous section we have put tremendous effort into establishing a theory of dimension of commutative rings. Let us take a look through our new looking glass at these concepts. The topological side of this dimension theory is easier than the algebraic side. So let us now introduce the notions fitting for the spectrum of a noetherian ring. In a Hausdorff space $(X, \mathcal{T})$ the irreducible components of X are of the form $\{\, x \,\}$ for some $x \in X$, so we get $\operatorname{tdim}(X) = 0$ and no new insights. But the spectrum of a ring is not hausdorff and this is where the theory will shine.

(8.95) Definition:

Let $(X, \mathcal{T})$ be a topological space, as in (8.94) let us denote the set of closed irreducible subsets of X by $\mathcal{I}(X)$ again. Then we define the **(topological) dimension** of X to be the maximal length of an ascending chain of closed, irreducible subsets of X. Formally we let $\operatorname{tdim}(\emptyset) := -1$ and if $X \neq \emptyset$, then

$$\operatorname{tdim}(X) \;:=\; \sup \left\{ d \in \mathbb{N} \;\middle|\; \begin{array}{l} \exists\, I_0, \ldots, I_d \in \mathcal{I}(X) \text{ such that} \\ I_0 \neq \emptyset \text{ and } I_0 \subset \ldots \subset I_d \end{array} \right\} \in \mathbb{N} \cup \{\infty\}$$

(8.96) Proposition: (viz. 1314)

Let $(X, \mathcal{T})$ be a topological space, $C \subseteq X$ be a closed and $U \subseteq X$ be an open subset of X. Then the following statements are true

(i) $\operatorname{tdim}(C) \leq \operatorname{tdim}(X)$ and $\operatorname{tdim}(U) \leq \operatorname{tdim}(X)$

(ii) If X is irreducible and $\operatorname{tdim}(X) < \infty$ finite-dimensional and $C \neq X$ even $\operatorname{tdim}(C) < \operatorname{tdim}(X)$

(iii) If $\operatorname{tdim}(X) < \infty$ is finite-dimensional, then the dimension of X equals the maximal dimension of its irreducible components, formally that is

$$\operatorname{tdim}(X) \quad = \quad \max\{\, \operatorname{tdim}(I) \mid I \in \operatorname{IRR}(X) \,\}$$

(8.97) Definition: (viz. 1314)
The topological space $(X, \mathcal{T})$ is said to be **noetherian**, iff one (and hence all) of the following five equivalent conditions is satisfied

(a) Every open subset U of X is compact in X, in the sense of (6.17).

$$P \subseteq X \text{ open} \quad \Longrightarrow \quad P \subseteq X \text{ compact}$$

(b) Every family of open subsets has a maximal element, i.e. for any non-empty set $\mathcal{U} \subseteq \mathcal{T}$ there is some $U^* \in \mathcal{U}$ such that for any $U \in \mathcal{U}$ we get the implication

$$U^* \subseteq U \quad \Longrightarrow \quad U^* = U$$

(c) Every set of closed subsets has a minimal element, i.e. for any non-empty set $\mathcal{C} \subseteq \{\, X \setminus U \mid U \in \mathcal{T} \,\}$ there is some $C_* \in \mathcal{C}$ such that for any $C \in \mathcal{C}$ we get the implication

$$C \subseteq C_* \quad \Longrightarrow \quad C = C_*$$

(d) Every ascending chain of open sets becomes stationary, that is: If $U_k \subseteq X$ is an open subset (where $k \in \mathbb{N}$) such that $U_0 \subseteq U_1 \subseteq \ldots \subseteq U_n \subseteq \ldots$ then there is some $n \in \mathbb{N}$ such that for any $k \in \mathbb{N}$ we get $U_{n+k} = U_n$.

(e) Every descending chain of closed sets becomes stationary, that is: If $C_k \subseteq X$ is a closed subset (where $k \in \mathbb{N}$) such that $C_0 \supseteq C_1 \supseteq \ldots \supseteq C_n \supseteq \ldots$ there is some $n \in \mathbb{N}$ such that for any $k \in \mathbb{N}$ we get $C_{n+k} = C_n$.

(8.98) Proposition: (viz. 1315)
Let $(X, \mathcal{T})$ be a noetherian topological space. A subset $L \subseteq X$ is said to be **locally closed**, iff it is of the form $L = U \cap C$ for some open set $U \subseteq X$ and some closed set $C \subseteq X$. And thereby we obtain

(i) X has only finitely many irreducible components, i.e. $\#\operatorname{IRR}(X) < \infty$.

(ii) If X is both, noetherian and hausdorff, then X already is a finite set $\#X < \infty$ and carries the discrete topology $\mathcal{T} = \mathcal{P}(X)$.

(iii) Any locally closed subset $L \subseteq X$ is compact.

(iv) Any locally closed subset $L \subseteq X$ becomes a noetherian topological space in the relative topology $\mathcal{T} \cap L$ it inherits from X.

(v) *Noetherian Induction:* Let φ be any property of the closed subsets of X, i.e. φ is a mapping of the form $\varphi : \{ X \setminus U \mid U \in \mathcal{T} \} \to \{ \text{true, false} \}$ such that $\varphi(\emptyset)$ and for any non-empty closed subset $D \subseteq X$ we get the induction hypothesis

$$\Big(\forall\, C \subseteq X \text{ closed, with } C \subset D : \varphi(C)\Big) \quad \Longrightarrow \quad \varphi(D)$$

then φ is already true for the entire space X, that is we also get $\varphi(X)$.

(8.99) Lemma: (viz. 1316) **Topological Laskar-Noether Theorem**
Let $(N, \mathcal{T})$ be a noetherian topological space and $X \subseteq N$ be a closed subset. Then there are uniquely determined $r \in \mathbb{N}$ and $X_1, \ldots, X_r \subseteq N$ such that the following statements (1), (2), (3) and (4) are true. And in this case we also obtain statement (5), where

(1) $X = X_1 \cup \cdots \cup X_r$

(2) $\forall\, i \neq j \in 1 \ldots r$ we get $X_i \not\subseteq X_j$

(3) $\forall\, i \in 1 \ldots r$ we get $X_i \subseteq X$ is closed

(4) $\forall\, i \in 1 \ldots r$ we get X_i is irreducible

(5) $\operatorname{IRR}(X) = \{ X_1, \ldots, X_r \}$

(8.100) Corollary: (viz. 1317)
Let $(X, \mathcal{T})$ be a noetherian topological space in which for any $x \in X$ the set $\{ x \} \subseteq X$ is closed (that is X is a so-called T_1-space). Then X is finite if and only if $\operatorname{tdim}(X) = 0$ and in this case the irreducible components are precisely the one-point sets $\operatorname{IRR}(X) = \{\{x\} \mid x \in X\}$

$$1 \leq \#X < \infty \quad \Longleftrightarrow \quad \operatorname{tdim}(X) = 0$$

(8.101) Example:
If $(F, +, \cdot)$ is any field, then the space $N := F^n$ is an irreducible, noetherian T_1-space in the Zariski-topology. And if $X \subseteq N$ is a closed set - that is $X = \mathbb{V}(\mathfrak{a})$ for some ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} F[t_1, \ldots, t_n]$, then by (8.99) X is a noetherian space in the relative topology, as well. The irreducible components of X are the $X_i = \mathbb{V}(\mathfrak{p}_i) \subseteq X$, where the $\mathfrak{p}_i \trianglelefteq_{\mathrm{i}} F[t_1, \ldots, t_n]$ are the prime ideals, that are minimal over $\mathfrak{a}$.

(8.102) Example:
Consider any field $(F, +, \cdot)$ and let us denote $R := F[t_k \mid k \in \mathbb{N}]$ the polynomial ring in countably many variables and $X := \operatorname{Spec}(R)$. Then R is *not* noetherian, since $\mathfrak{p}_k := \langle t_0, \ldots, t_k \rangle_{\mathrm{i}} \trianglelefteq_{\mathrm{i}} R$ forms a strictly ascending chain $\mathfrak{p}_0 \subset \mathfrak{p}_2 \subset \ldots$ of prime ideals. Consequently $I_k := \mathbb{V}(\mathfrak{p}_k)$ forms a strictly descending chain $I_0 \supset I_1 \supset I_2 \supset \ldots$ of closed, irreducible subsets. That is X is not a noetherian topological space. But as R is an integral domain X is an irreducible topological space: $X = \mathbb{V}(0)$ and 0 is a minimal prime ideal of R. That is X is the one and only irreducible component $\operatorname{IRR}(X) = \{ X \}$ of X. In particular there are topological spaces with finitely many irreducible components that are *not* noetherian.

(8.103) Theorem: (viz. 1317)
Let $(X, \mathcal{T})$ be a noetherian topological space, then the irreducible components are a refinement of the connected components of X in the following sense: First of all X only has finitely many connected components. More precisely it cannot have more connected components than irreducible components

$$\#\mathrm{cnc}(X) \;\leq\; \#\mathrm{irr}(X) \;<\; \infty$$

And the connected components induce a partition of the irreducible components in the following way: For any connected component $K \in \mathrm{cnc}(X)$ let us denote $\mathcal{I}(K) := \{\, I \in \mathrm{irr}(X) \mid I \subseteq K \,\}$ the set of all irreducible components inside K. Then the $\mathcal{I}(K)$ are pairwise disjoint (i.e. for any $K, L \in \mathrm{cnc}(X)$ we get $\mathcal{I}(K) \cap \mathcal{I}(L) \neq \emptyset \implies K = L$) and we get the identiites

$$\begin{aligned} \mathrm{irr}(X) &= \bigcup \{\, \mathcal{I}(K) \mid K \in \mathrm{cnc}(X) \,\} \\ K &= \bigcup \mathcal{I}(K) \end{aligned}$$

8.9 Regular Local Rings

In algebraic geometry one is interested in the dimension of a variety X in one of its points $x \in X$. This can be gleaned by using the ring of regular local functions $\mathcal{O}_x(X)$ as a looking glass, which is a local ring. So in this section we study the dimension of localisations of rings an specifically local rings. In a *regular* point $x \in X$ the dimension of the tangent space agrees with the local dimension of X, e.g. a line is the tangent space at a point on a plane curve. But if the curve intersects with itself there are two linearly independent tangent vectors at the junction. That is the dimension of the tangent space may jump up at certain points, that are called *singular* points of X. We would like to identify and manage such singular points.

(8.104) Proposition: (viz. 1318)
Let $(R, +, \cdot)$ be a local, noetherian ring with maximal ideal $\mathfrak{m}$ and denote the *residue field* of R modulo $\mathfrak{m}$ by $E := R/\mathfrak{m}$. We now regard $\mathfrak{m}$ as an R-module, then $\mathfrak{m}/\mathfrak{m}^2$ becomes an E-vector space under the following scalar multiplication:

$$(a + \mathfrak{m})(m + \mathfrak{m}^2) \;:=\; (am) + \mathfrak{m}^2$$

As $\mathfrak{m}$ also is an R-module we may look at the number of generators required for $\mathfrak{m}$, that is elements $m_1, \ldots, m_n \in R$ such that $\mathfrak{m} = Rm_1 + \cdots + Rm_n$. Thereby we find that for any elements $m_1, \ldots, m_n \in R$ the following two statements are equivalent

(a) $\{ m_1, \ldots, m_n \}$ generates $\mathfrak{m}$ as an R-module

(b) $\{ m_1 + \mathfrak{m}^2, \ldots, m_n + \mathfrak{m}^2 \}$ generates $\mathfrak{m}/\mathfrak{m}^2$ as an E-vector-space

Recall that the minimal number of generators requires for $\mathfrak{m}$ is called the *rank* of $\mathfrak{m}$, denoted by $\operatorname{rank}_R(\mathfrak{m})$. Then we find that this number equals the dimension of $\mathfrak{m}/\mathfrak{m}^2$ as an E-vector-space:

$$\dim_E \left(\mathfrak{m} \Big/ \mathfrak{m}^2 \right) \;=\; \operatorname{rank}_R(\mathfrak{m})$$

(8.105) Remark: $(\diamondsuit)$
We want to append a word on the geometric idea behind $\mathfrak{m}/\mathfrak{m}^2$, without going into details, as this is a theory of its own. In algebraic geometry we regard the ring $\mathcal{O}_x(X)$ of local regular functions of a variety X. These are functions $r : U \subseteq X \to \mathbb{F}$ that are defined on a dense open subset $x \in U \subseteq X$ that can locally be written as the quotient of polynomial functions. They build up a local ring with maximal ideal $\mathfrak{m}_x(X)$ of those local regular functions, that vanish $r(x) = 0$ at x. Thinking of a Taylor expansion of r the residue class $r + \mathfrak{m}_x(X)^2$ is the linear part of r (it has no constant term, as $r(x) = 0$ and the higher order terms are eaten up by $\mathfrak{m}_x(X)^2$). What remains is the linear freedom a local regular function can have at x. Thus $\mathfrak{m}_x(X)/\mathfrak{m}_x(X)^2$ is the (co)tangential space of X at the point $x \in X$. Therefore its dimension is (apart from singularities) the dimension of X itself. And the above proposition ascertains, that this is just the same, as the minimal number of generators needed for $\mathfrak{m}_x(X)$.

(8.106) Proposition: (viz. 1319)
Let $(R,+,\cdot)$ be a local ring with maximal ideal $\mathfrak{m}$. Suppose $\operatorname{kdim}(R) < \infty$ is finite-dimensional, then for any prime ideal $\mathfrak{p} \in \operatorname{Spec}(R)$ we find the following equivalence

$$\mathfrak{p} = \mathfrak{m} \iff \operatorname{height}(\mathfrak{p}) = \operatorname{height}(\mathfrak{m})$$

(8.107) Lemma: (viz. 1319)
Let $(R,+,\cdot)$ be a noetherian, local ring with maximal ideal $\mathfrak{m}$. Then the Krull-dimension of R cannot exceed the minimal number of generators required for $\mathfrak{m}$, that is we find

$$\operatorname{kdim}(R) = \operatorname{height}(\mathfrak{m}) \leq \operatorname{rank}(\mathfrak{m}) < \infty$$

and the Krull-dimension equals the minimal number d of elements $a_1,\ldots,a_d$ of R such that $\mathfrak{m}$ is a prime ideal minimal over the ideal $\mathfrak{a} := a_1R + \cdots + a_dR$. Formally that is the identity

$$\operatorname{kdim}(R) = \min\left\{ d \in \mathbb{N} \;\middle|\; \begin{array}{l} \exists\, a_1,\ldots,a_d \in R \text{ such that} \\ a_1R + \cdots + a_dR \subseteq \mathfrak{m} \text{ is minimal} \end{array} \right\}$$

Nota by (2.139) the property that "$\mathfrak{m}$ is a minimal prime ideal over $\mathfrak{a}$" can be formulated in many different ways. A commonly used alternative is $\mathbb{V}(\mathfrak{a}) = \{\mathfrak{m}\}$.

Let $a_1,\ldots,a_d \in R$ such that $\mathfrak{m}$ is a minimal prime ideal over $\mathfrak{a} := \langle a_1,\ldots,a_d\rangle_{\mathfrak{i}}$. It may happen that these elements do not generate $\mathfrak{m}$ as an R-module, that we need some more $\mathfrak{m} = \langle m_1,\ldots,m_n\rangle_{\mathfrak{i}}$. Then the above propositions tell us that the difference in the dimensions n of the cotangent space $\mathfrak{m}/\mathfrak{m}^2$ and the dimension d of R is derived from those elements that were missing to build up $\mathfrak{m}$. A neat special case is $n = d$, that is when the $a_1,\ldots,a_d$ are already sufficient, to build up $\mathfrak{m}$.

(8.108) Definition:
If $(R,+,\cdot)$ is a local ring, having the maximal ideal $\mathfrak{m}$, then a subset of elements $\{a_1,\ldots,a_d\} \subseteq R$ are said to be a **local system of parameters** of R, iff it satisfies the following two properties

(1) $d = \operatorname{kdim}(R)$

(2) $\mathfrak{m}$ is a minimal prime ideal over $a_1R + \cdots + a_dR$

A commutative ring $(R,+,\cdot)$ is said to be a **regular local ring**, iff (1) R is a local ring, (2) R is a noetherian ring and (3) if $\mathfrak{m}$ is the maximal ideal of R, then $\operatorname{kdim}(R) = \operatorname{rank}(\mathfrak{m})$.

Nota if R is a noetherian, local ring, then R has a local system of parameters, by (8.107). And if R is a regular local ring and $\mathfrak{m} = m_1R + \cdots + m_nR$, where $n = \operatorname{rank}(\mathfrak{m})$ is minimal, then $\{m_1,\ldots,m_n\}$ is a local system of parameters of R.

(8.109) Proposition: (viz. 1319)
Let $(R,+,\cdot)$ be a local, noetherian ring with maximal ideal $\mathfrak{m}$ and consider some elements $a_1,\ldots,a_m \in \mathfrak{m}$ and let us denote $\mathfrak{a} := a_1R + \cdots + a_mR$. Then the following statements are true

(i) The quotient ring $R/\mathfrak{a}$ is a noetherian, local ring with maximal ideal $\mathfrak{m}/\mathfrak{a}$ and the Krull-dimension of this ring is at least
$$\operatorname{kdim}\left(R\Big/\mathfrak{a}\right) \;\geq\; \operatorname{kdim}(R) - m$$

(ii) If $a_{m+1},\ldots,a_n \in \mathfrak{m}$ are elements, such that $\{\, a_1,\ldots,a_n \,\}$ is a local system of parameters of R, then $\mathfrak{m}/\mathfrak{a}$ is a prime ideal, minimal over $\langle a_{m+1}+\mathfrak{a},\ldots,a_n+\mathfrak{a}\rangle_{\mathfrak{i}}$.

(iii) The set $\{\, a_1,\ldots,a_m \,\}$ can be extended to a local system of parameters of R if and only if the Krull-dimension of $R/\mathfrak{a}$ is equal to $\operatorname{kdim}(R/\mathfrak{a}) = \operatorname{kdim}(R) - m$.

(iv) If $\operatorname{height}(\mathfrak{a}) = m$, then (1) $\{\, a_1,\ldots,a_m \,\}$ can be extended to a local system of parameters $\{a_1,\ldots,a_n\}$ (where $n = \operatorname{kdim}(R) \geq m$) of R and thereby (2) $\{a_{m+1}+\mathfrak{a},\ldots,a_n+\mathfrak{a}\}$ is a local system of parameters of $R/\mathfrak{a}$, as we also have (3) $\operatorname{kdim}(R) = \operatorname{kdim}(R/\mathfrak{a}) + \operatorname{height}(\mathfrak{a})$.

(8.110) Example:
Let $(E,+,\cdot)$ be a field and regard the ideal $\mathfrak{a} := t^3E[t]$ in the polynomial ring $E[t]$. Then we study the ring $R := E[t]/\mathfrak{a}$ and find that it features the following properties

- By construction any polynomial $f \in E[t]$ is reduced to $f[2]t^2 + f[1]t + f[0] + \mathfrak{a}$ and hence we can explicitly write R as the set $R = \left\{\, a_2t^2 + a_1t + a_0 + \mathfrak{a} \mid a_0,a_1,a_2 \in E \,\right\}$. As this representation is unique 1, x and x^2 build up an E-basis of $R:E$, where $x := t+\mathfrak{a}$, and hence $[R:E] = 3$.

- Note that $E[t]$ is a PID and by the correspondence theorem of ideals in quotients the ideal $\mathfrak{b}/\mathfrak{a}$ of R has its origin in an ideal $\mathfrak{b} = gE[t]$. Hereby $t^3E[t] \subseteq gE[t]$ turns into $g \mid t^3$ and therefore R has the following 4 ideals, precisely
$$\operatorname{Ideal}(R) \;=\; \left\{\, 0,\, x^2R,\, xR,\, R \,\right\}$$

- Of these ideals $\mathfrak{m} := xR$ is the only prime ideal and this already is maximal. That is R is a local ring and $\operatorname{Spec}(R) = \operatorname{Smax}(R)$. In particular $\operatorname{kdim}(R) = 0$. As R also in noetherian (any ideal is generated by a single element) it even is an artinian ring.

- The maximal ideal $\mathfrak{m}$ of R is of the form $\mathfrak{m} = \left\{\, a_2x^2 + a_1x \mid a_1,a_2 \in E \,\right\}$. In particular $\operatorname{rank}(\mathfrak{m}) = 1$, as $\mathfrak{m} = xR$ and $\{x\}$ is a minimal generating set of $\mathfrak{m}$. From this we see R is local and noetherian, but $\operatorname{kdim}(R) = 0 < 1 = \operatorname{rank}(\mathfrak{m})$. This means that R is *not* a regular local ring.

- Let us take a look at the cotangent space $\mathfrak{m}/\mathfrak{m}^2$: As $\mathfrak{m} = xR$ clearly $\mathfrak{m}^2 = x^2R$. Thus the elements of $\mathfrak{m} = \left\{\, a_2x^2 + a_1x \mid a_1,a_2 \in E \,\right\}$ loose their x^2-part, it only remains
$$\mathfrak{m}\Big/\mathfrak{m}^2 \;=\; \left\{\, a_1x + \mathfrak{m}^2 \mid a_1 \in E \,\right\}$$
Thus $\mathfrak{m}/\mathfrak{m}^2$ is a 1-dimensional vector space with basis $x+\mathfrak{m}^2$. The above proposition (8.104) tells us, that this is no coincidence, but a general truism.

regular sequences, [Matrsumura Theorem 36] complete intersection ring = every prime ideal satisfies height($\mathfrak{p}$) = rank($\mathfrak{p}$) Auslander-Buchsbau Theorem: any regular local ring is an UDF [Matrsumura Theroem 48] Richard E Borcherds (youtube) for examples

8.10 Hilbert-Samuel Polynomial

Hilbert-Samuel polynomial Poincaré series Hilbert-Serre theorem Artin-Rees lemma

Chapter 9

Group Theory

9.1 Basic Notions

normal subgroups, kernel+image, isomorphism theorems, quotient groups

(9.1) Example: (viz. 643)
Consider a metric space (Y,d) and a non-empty subset $\emptyset \neq X \subseteq Y$, then a map $f : X \to X$ is called a **symmetry** of X, if it reaches all points and preserves distance. That is iff

(1) f is surjective

(2) for any $x, y \in X$ we get $d(f(x),f(y)) = d(x,y)$

The set of all symmetries of X will be denoted by $\mathrm{sym}(X)$ and in fact this is a sub-group of of the permutation-group of X. That is any symmetry already is bijective and $\mathrm{sym}(X)$ is closed under composition and taking inverse.

$$\mathrm{sym}(X) \quad \leq_{\mathrm{g}} \quad S_X$$

Proof of (9.1):
First of all, we need to show that any symmetry $f : X \to X$ is injective: So pick up any $x, y \in X$ and assume $f(x) = f(y)$. As f preserves distance this would mean $0 = d(f(x),f(y)) = d(x,y)$ and hence $x = y$. This already is the injectivity.
It is also clear, that $\mathbb{1}_X \in \mathrm{sym}(X)$. And if f and g are symmetries of X, then we have $d(g(x),g(y)) = d(x,y)$ and $d(f(u),f(v)) = d(u,v)$ for any u, v, x and $y \in X$. Let us take $x = f(u)$ and $y = f(v)$ then we see

$$d\big(gf(u),gf(v)\big) \;=\; d\big(g(x),g(y)\big) \;=\; d\big(x,y\big) \;=\; d\big(f(u),f(v)\big) \;=\; d\big(u,v\big)$$

such that $gf \in \mathrm{sym}(X)$ again, as gf also is surjective. As f is invertible we also get $u = f^{-1}(x)$ and $v = f^{-1}(y)$ such that we also find $f^{-1} \in \mathrm{sym}(X)$ (and hence $\mathrm{sym}(X)$ is a group contained in S_X) from the equation

$$d\big(f^{-1}(x),f^{-1}(y)\big) \;=\; d\big(u,v\big) \;=\; d\big(f(u),f(v)\big) \;=\; d\big(x,y\big)$$

□

conjugation, sylow theorems, p-q theorem, ordered groups, representation theory, invariant theory

9.2 Group Actions

(9.2) Definition:
Let $(G, \circ)$ be a group and X be an arbitrary set, then a map $\mu : G \times X \to X$ (written as $\mu : (g, x) \mapsto gx$) is said to be an **operation** of G on X, iff it satisfies one of the following two equivalent conditions

(a) $G \to S_X : g \mapsto T_g$ where $T_g : X \to X : x \mapsto gx$ is a group-homomorphism

(b) $\forall\, g, h \in G$ and $\forall\, x \in G$ we get the properties $ex = x$ and $(gh)x = g(hx)$

And in this case we define the following notions: for any $x \in X$ we define the **orbit** $Gx \subseteq X$ and the **stabilizer** $G^x \subseteq G$. And for any $g \in G$ we also define the **fixed point set** $X^g \subseteq X$ and the set X^G of **invariants**

$$\begin{aligned} Gx &:= \{\, gx \mid g \in G \,\} \\ G^x &:= \{\, g \in G \mid gx = x \,\} \\ G^X &:= \{\, g \in G \mid \forall\, x \in X : gx = x \,\} \\ X^g &:= \{\, x \in X \mid gx = x \,\} \\ X^G &:= \{\, x \in X \mid \forall\, g \in G : gx = x \,\} \end{aligned}$$

Finally a subset $A \subseteq X$ is said to be G-**invariant** iff for any $g \in G$ we get

$$gA := \{\, gx \mid x \in A \,\} \subseteq A$$

(9.3) Example:

(i) If $X \neq \emptyset$ is any non-empty set then any subgroup $S \leq_{\mathfrak{g}} S_X$ of the permutation group S_X operates on X in a most obvious way

$$S \times X \to X \;:\; (\sigma, x) \mapsto \sigma(x)$$

(ii) By (1.12.(ii)) any group G operates on itself, by multiplication from the left, that is we get an operation on G by

$$G \times G \to G \;:\; (g, h) \mapsto gh$$

(iii) Finally any group G operates on itself by *conjugation*, that is we obtain another action of G on G by letting

$$G \times G \to G \;:\; (g, h) \mapsto h^g := ghg^{-1}$$

Prob first of all it is clear that for any $x \in G$ we have $x^e = exe^{-1} = x$. Also for any $g, h \in G$ we can compute $x^{gh} = (gh)x(gh)^{-1} = ghxh^{-1}g^{-1} = g(x^h)g^{-1} = (x^h)^g$, so that both properties are satisfied.

(9.4) Proposition: (viz. 706)

(i) It is easy to see that an operation $G \times X \to X$ defines an equivalence relation on X by letting $x \sim y \;:\Longleftrightarrow\; \exists\, g \in G : y = gx$. And the equivalence classes of this relation clearly are the orbits

Gx. The quotient set of X under this relation is denoted by

$$X\big/_G \;:=\; \{\, Gx \mid x \in X \,\}$$

(ii) It also is immedeately clear that the stabilizer $G^x \leq_g G$ is a subgroup of G. Another well-known fact is the following 1-to-1 correspondence

$$Gx \longleftrightarrow G\big/_{G^x} \;:\; gx \mapsto gG^x$$

(iii) If $A \subseteq X$ is G-invariant, then for any $g \in G$ we have $gA = A$. And we can thereby restrict ϱ to an operation of G on A, that is

$$\varrho \;:\; G \times A \to A \;:\; (g,x) \mapsto gx$$

(iv) If A is G-invariant, then the complement $X \setminus A$ is G-invariant, too.

(v) **Orbit Formulas**: If $(G,\circ)$ is a finite group, that operates on the finite set X, then (for any $x \in X$) the following equations are true

$$\begin{aligned} \#Gx &= \frac{\#G}{\#G^x} \\ \#X &= \#G \cdot \sum_{Gx \in X/G} \frac{1}{\#G^x} \end{aligned}$$

(vi) **Formula of Burnside**: If $(G,\circ)$ is a finite group, that operates on the finite set X, then the following equation holds true

$$\#G \cdot \#X\big/_G \;=\; \sum_{g\in G} \#X^g \;=\; \sum_{x\in X} \#G^x$$

(9.5) Definition:
Let $(G,\circ)$ be a group and $(\mathbb{F},+,\cdot)$ be any field. Now a group-homomorphism $\chi : G \to \mathbb{F}^*$ from G to the multiplicative group $\mathbb{F}^*$ is called a **character** of G.

(9.6) Proposition: (viz. 646)
Let $(G,\circ)$ be any group and $(\mathbb{F},+,\cdot)$ be any field. If now $\chi_1,\ldots,\chi_r : G \to \mathbb{F}^*$ are pairwise distinct characters of G (i.e. for any $i \neq j \in 1\ldots r$ we have $\chi_i \neq \chi_j$) then the set $\{\,\chi_1,\ldots,\chi_r\,\} \subseteq \mathcal{F}(G,\mathbb{F})$ already is $\mathbb{F}$-linear independent (as $\mathbb{F}$-valued functions).

(9.7) Definition:
Let $(G,\circ)$ be any group and R be a commutative ring. Then $\mu : G \times R \to R$ is said to be an **algebraic operation**, iff we get the properties

(1) $\mu : G \times R \to R$ is an operation of G on R

(2) for any $g \in G$ the map $T_g : R \to R : a \mapsto ga$ is a homomorphism

And in this case we define the **invariant ring** under the operation μ to be

$$R^G \;:=\; \{\, a \in R \mid \forall\, g \in G : ga = g \,\}$$

Nota as T_g is bijective with $T_g^{-1} = T_{g^{-1}}$ we find that (2) already implies that any T_g even is an automorphism of the ring R. And it is immediately clear that the invariant ring $R^G \leq_{\mathrm{r}} R$ is a sub-ring of R.

(9.8) Proposition: (viz. 648)
Let G be a group, R be a commutative ring and A be a commutative monoid. If now $\mu : G \times R \to R$ is an algebraic operation, then this canonically induces an algebraic operation $G \times R[A] \to R[A]$ on the group ring $R[A]$, by

$$G \times R[A] \to R[A] \;:\; (g, f) \mapsto \sum_{\alpha \in A} (gf[\alpha])t^{\alpha}$$

And for this operation we obtain the following identity of the invariant rings

$$R[A]^G \;=\; R^G[A]$$

(9.9) Proposition: (viz. 647)
Let $G \times R \to R : a \mapsto ga$ be an algebraic operation of the group G on the commutative ring R. Let now $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ be any ideal, then we get

(i) $\mathfrak{a}^G := \{\, a \in \mathfrak{a} \mid \forall\, g \in G : ga = a \,\} = \mathfrak{a} \cap R^G \trianglelefteq_{\mathrm{i}} R^G$

(ii) If $\mathfrak{a}$ is an G-invariant ideal (that is $g\mathfrak{a} \subseteq \mathfrak{a}$ for any $g \in G$) then we obtain an algebraic operation of G on the quotient ring, via

$$G \times {}^{R}\!\Big/_{\mathfrak{a}} \to {}^{R}\!\Big/_{\mathfrak{a}} \;:\; (g, b + \mathfrak{a}) \mapsto gb + \mathfrak{a}$$

(iii) And in case $\mathfrak{a}$ is an G-invariant ideal, then we obtain a well-defined, injective homomorphism of rings by virtue of

$$R^G \Big/_{\mathfrak{a}^G} \hookrightarrow \left({}^{R}\!\Big/_{\mathfrak{a}}\right)^G \;:\; b + \mathfrak{a}^G \mapsto b + \mathfrak{a}$$

(9.10) Proposition: (viz. 647)
Let $G \times X \to X : (g, x) \mapsto gx$ be a group operation and let R be a commutative ring. Further consider $A := \mathcal{F}(X, R)$ the R-algebra of functions from X to R. Then we obtain an algebraic operation of G on A by letting

$$G \times A \to A \;:\; (g, f) \mapsto \big(x \mapsto f(g^{-1}x)\big)$$

And if $M \subseteq X$ is a G-invariant subset (that is $gM \subseteq M$ for any $g \in G$), then $\mathbb{I}(M) := \{\, f \in A \mid \forall\, x \in M : f(x) = 0 \,\}$ is a G-invariant ideal (that is $\mathbb{I}(M) \trianglelefteq_{\mathrm{i}} A$ is an ideal and $g\mathbb{I}(M) \subseteq \mathbb{I}(M)$ for any $g \in G$). And in this case we finally we obtain the isomorphy

$$A^G \Big/_{\mathbb{I}(M)^G} \;\xrightarrow{\sim}\; \left(A \Big/_{\mathbb{I}(M)}\right)^G \;:\; f + \mathbb{I}(M)^G \mapsto f + \mathbb{I}(M)$$

Proof of (9.6):
If $r = 1$ then the linear independance is clear, as $\chi_1 \neq 0$. So pick up the minimal number $k \geq 2$ such that there are $a_1 \ldots, a_k \in \mathbb{F}^*$ and (pairwise distinct) $i_1, \ldots, i_k \in 1 \ldots r$ satisfying

$$a_1\chi_{i_1} + \cdots + a_k\chi_{i_k} \;=\; 0$$

renumbering the χ_i we may assume $i_1 = 1$ and $i_2 = 2$ and so on until $i_k = k$. Let us now denote $b_i := a_i/a_k$ then we obtain the central equation

$$\sum_{i=1}^{k-1} b_i\chi_i + \chi_k \;=\; 0$$

As $\chi_1 \neq \chi_k$ (remember $k \geq 2$) there is some $h \in G$ such that $\chi_1(h) \neq \chi_k(h)$. For any $g \in G$ let us now insert gh into the central equation, this yields

$$\sum_{i=1}^{k-1} b_i\chi_i(g)\chi_i(h) + \chi_k(g)\chi_k(h) \;=\; 0$$

On the other hand (for any $g \in G$ we may first insert g into the central equation and afterwards multiply with $\chi_k(h)$. This yields another equation

$$\sum_{i=1}^{k-1} b_i\chi_i(g)\chi_k(h) + \chi_k(g)\chi_k(h) \;=\; 0$$

Subtraction these two equations we obtain another identity (for any $g \in G$)

$$\sum_{i=1}^{k-1} b_i\big(\chi_k(h) - \chi_k(h)\big)\chi_i(g) \;=\; 0$$

As any $c_i := b_i(\chi_k(h) - \chi_k(h)) \in \mathbb{F}$ is scalar we have found a linear dependence with *fewer* that k elements. As k has been minimal this can only be if $c_i = 0$ for any $i \in 1 \ldots (k-1)$. But by construction we have $c_1 \neq 0$, a contradiction. Thus k could not have be chosen in the first place and this is just the linear independence of the χ_i. □

Proof of (9.9):

(i) From the definition of $\mathfrak{a}^G$ it is clear that $\mathfrak{a}^G = \mathfrak{a} \cap R^G$. Yet $R : R^G$ is a ring extension and hence it is a general fact that $\mathfrak{a} \cap R^G \trianglelefteq_{\mathfrak{i}} R^G$.

(ii) We first prove the well-definedness of the operation: consider b, $b' \in R$ with $b + \mathfrak{a} = b' + \mathfrak{a}$. That is $b' - b \in \mathfrak{a}$ and hence (as $\mathfrak{a}$ is G-invariant) $gb' - gb = g(b' - b) \in g\mathfrak{a} \subseteq \mathfrak{a}$. And this again yields $gb + \mathfrak{a} = gb' + \mathfrak{a}$. Now as $b \mapsto gb + \mathfrak{a}$ is nothing but the composition of $b \mapsto gb \mapsto gb + \mathfrak{a}$ we also find that $b + \mathfrak{a} \mapsto gb + \mathfrak{a}$ is a homomorphism. That is the operation even is algebraic.

(iii) Let us first consider $R^G \to (R/\mathfrak{a})^G : b \mapsto b + \mathfrak{a}$. This clearly is a well-dfined homomorphism as $g(b + \mathfrak{a}) = gb + \mathfrak{a} = b + \mathfrak{a}$. And the kernel of this homomorphism clearly is $\{\, b \in R^G \mid b \in \mathfrak{a} \,\} = \mathfrak{a} \cap R^G = \mathfrak{a}^G$. Hence the map in the claim is well-defined and injective.

□

Proof of (9.10):
As $ef(x) = f(e^{-1}x) = f(x)$ we clearly have $ef = f$ for any $f \in A$. And given g, $h \in G$, $f \in A$ and $x \in X$ it is straightforward to compute

$$(h(gf))(x) \;=\; (gf)(h^{-1}x) \;=\; f(g^{-1}h^{-1}x) \;=\; f((gh)^{-1}x) \;=\; ((gh)f)(x)$$

Thus $G \times A \to A$ is a group action. And the operations of A are point-wise it is clear that this operation also is algebraic. Next we prove that $\mathbb{I}(M)$ is a G-invariant ideal. The properties of an ideal are immediatley clear. Let us consider $f \in \mathbb{I}(M)$, $g \in G$ and any $x \in M$. As M is G-invariant we get $g^{-1}x \in g^{-1}M \subseteq M$. And as $f \in \mathbb{I}(M)$ this yields $(gf)(x) = f(g^{-1}x) = 0$. As x has been arbitrary, this proves $gf \in \mathbb{I}(M)$, which also yields the G-invariance $g\mathbb{I}(M) \subseteq \mathbb{I}(M)$. It remains to prove

$$A^G \Big/ \mathbb{I}(M)^G \;\xrightarrow{\sim}\; \left(A \Big/ \mathbb{I}(M)\right)^G \;:\; f + \mathbb{I}(M)^G \mapsto f + \mathbb{I}(M)$$

We have already proved the well-definedness and injectivity of this map in (9.10). For the surjectivity we are given some $f + \mathbb{I}(M)$ which is G-invariant. That is $gf + \mathbb{I}(M) = f + \mathbb{I}(M)$ for any $g \in G$. In other words that is $f(g^{-1}x) = (gf)(x) = f(x)$ for any $g \in G$. Let us denote $1_M : X \to R$ the characteristic function of M and let $\widetilde{f} := 1_M f$. If $x \notin M$ then we clearly have $\widetilde{f}(x) = 1_M(x)f(x) = 0$. And as $X \setminus M$ is G-invariant as well, we get $1_M(g^{-1}x) = 0$ and hence $(g\widetilde{f})(x) = \widetilde{f}(g^{-1}x) = 1_M(g^{-1}x)f(x) = 0$, too. Thus $\widetilde{f}(x) = 0 = g\widetilde{f}(x)$ for any $x \in X \setminus M$. Conversely if $x \in M$ then $1_M(x) = 1 = 1_M(g^{-1}x)$ which yields $g\widetilde{f}(x) = \widetilde{f}(g^{-1}x) = 1_M(g^{-1}x)f(g^{-1}x) = f(g^{-1}x) = (gf)(x) = f(x) = 1_M(x)f(x) = \widetilde{f}(x)$ as $x \in M$. Altogether we have proved $\widetilde{f} = g\widetilde{f}$, (for any $x \in X$) which is the G-invariance of $\widetilde{f}$. And we have already seen that $\widetilde{f}(x) = f(x)$ for any $x \in M$. But we have also seen, that $\widetilde{f} + \mathbb{I}(M) = f + \mathbb{I}(M)$, which means nothing but $\widetilde{f} + \mathbb{I}(M)^G \mapsto f + \mathbb{I}(M)$ under the map in question. □

Proof of (9.8):
We will first prove that $G \times R[A] \to R[A]$ truly is a group action. To do this consider any g and $h \in\in G$ and any $f \in R[A]$. By definition we clearly have $ef = f$. And further we find

$$g(hf) \;=\; g\left(\sum_{\alpha\in A}(hf[\alpha])t^\alpha\right) \;=\; \sum_{\alpha\in A} g(hf[\alpha])t^\alpha \;=\; \sum_{\alpha\in A}(gh)f[\alpha]t^\alpha \;=\; (gh)f$$

From the homomorphism property of $R \to R : a \mapsto ga$ we find that $(g, f) \mapsto gf$ truly is an algebraic operation (we omit tedious computations). So it only remains to prove $R[A]^G = R^G[A]$. The inclusion " $\supseteq$ " is trivial. Conversely consider any $f \in R[A]^G$. Then we have to show that for any $\alpha \in A$ and any $g \in G$ we get $gf[\alpha] = f[\alpha]$. Yet to see this it suffices to compare coefficients

$$\sum_{\alpha\in A}(gf[\alpha])t^\alpha \;=\; gf \;=\; f \;=\; \sum_{\alpha\in A} f[\alpha]t^\alpha$$

□

9.3 Some Number Theory

number theoretic functions Euler's φ-function Euler's σ-function

9.4 Representation Theory

Chapter 10

Homological Algebra

Consider a module M over a (not necessarily commutative) ring $(R, +, \cdot)$. To say that M is *finitely generated* means that there are finitely many elements m_1 to $m_n \in M$ such that any $x \in M$ can be written in the form $x = \sum_j b_j m_j$ for some $b_i \in R$. In other words iff the following homomorphism is surjective

$$\mu \ : \ R^n \twoheadrightarrow M \ : \ (b_1, \ldots, b_n) \mapsto \sum_{j=1}^{n} b_j m_j$$

In the language of chains of homomorphisms this can be put as: The chain $R^n \to M \to 0$ of module homomorphisms is exact. In order to have a more accurate description of M it would be nice to also know the kernel of μ.

In fact this is the question: 'Which $b \in R^n$ yield $\sum_j b_j m_j = 0$?' which amounts to a system of linear equations. We will concern ourselves in section 4.3 with solving these, but the best we can hope for is finding a parametrisation of $\ker(\mu)$. That is we want to have some base vectors k_1 to $k_m \in R^m$ such that $\mu(b) = 0$ if and only if $b = a_1 k_1 + \cdots + a_m k_m$ for some a_1 to $a_m \in R$. In turn $\ker(\mu)$ is the image of another homomorphism $\kappa : R^m \to R^n : (a_1, \ldots, a_m) \mapsto \sum_i a_i k_i$. In the language of chains of homomorphisms again, this is the exactness of

$$R^m \xrightarrow{\kappa} R^n \xrightarrow{\mu} M \to 0$$

A module M that allows such a chain is truly well-displayed, as the first isomorphism theorem of modules then allows to describe it, in the form

$$R^n \Big/ _{\mathrm{im}(\kappa)} \xrightarrow{\sim} M \ : \ b + \mathrm{im}(\kappa) \mapsto \sum_{j=1}^{n} b_j m_j$$

(10.1) Definition:
Let $(R, +, \cdot)$ be an arbitrary ring and M be an R-module. Then M is said to **admit a finite free presentation** (or simply to be **finitely presented**) iff there are integers m, $n \in \mathbb{N}$ such that there is an exact chain of module homomorphisms of the form

$$R^m \to R^n \to M \to 0$$

10.1 Diagram Chasing

snake-lemma et al

10.2 Projective Modules

AW (6.3) projective modules over PID are free
and injective modules - wikipedia!

10.3 Flat Modules

10.4 Homology Modules

chain (co)complexes, (co)homology modules, (co)homology morphisms, examples

10.5 Differentials

Matsumura - commutative ring theory - chapter 9

Chapter 11

Categorial Algebra

11.1 Categories

Generally speaking, algebra provides the structural concepts for all other fields of mathematics: Rings are the general concept of the base numbers, vector spaces are the general concept of function spaces and tangent spaces, algebras and derivations appear in calculus and so on. But you, the reader, probably noticed similarities, like homomorphisms have kernels or the existence of direct sums and products. Hence it makes sense to attempt a *second structurisation* that shall unify all these separate concepts in a general way. What we want to do here is introduce the concept of a *category*, that is a one-size-fits-all approach to all these different structures that allows to study their similarities in a general setting.

Hence we will define what we mean by a category and present the most fundamental examples of specific categories after that. The most prominent example is the category of sets - that is the entity of all sets. But it does not make sense to speak of the *set of sets*, say

$$\Omega \;:=\; \{\, X \mid X \text{ is a set} \,\}$$

This Ω is also called the **universe** in mathematics. However, if it was a set again, then we had $\Omega \in \Omega$ which not only is contra-intuitive (as we needed Ω to build up Ω in the first place), but can also lead to contradictions - the hell of mathematics. The solution is simple: We need a different name for arbitrary large collections of sets - let us call them *classes*.

In this chapter we will use the term *class* naively: A **class** is any collection of sets, with no restriction imposed on which or how many there are. As such a class need not be a set, any set is a class, but not every class is a set. A class that can also be build up as a set is said to be a **small** class. E.g. any set is a small class. A class that cannot be build up by set-theoretic constructions is called a **proper** class. E.g. the universe Ω above is a proper class.

You may think of a class as an expression of the form $\{\, X \mid \varphi(X) \,\}$ where $\varphi(X)$ is any expression of set theory concerning the variable symbol X. We have given a formal approach to classes, using the NBG axioms and a formal language with two variables (one for sets, the other for classes). And we have included a comment on alternative approaches to classes, at the end of this section, for the interested reader. But actually we recommend to use the term *class* naively, thinking of an arbitrary collection of sets, that might be too large to be a set itself.

(11.1) Definition:
A **category** is a triple $\mathcal{C} = (\mathcal{X}, \mathcal{M}, \circ)$ consisting of three classes $\mathcal{X}$, $\mathcal{M}$ and $\circ$ of the following form, that satisfy the properties (C1) and (C2) below:

- $\mathcal{X}$ is just any class, called the **objects** of the category $\mathcal{C}$ which we will also denote by $\mathrm{obj}(\mathcal{C}) := \mathcal{X}$. If $\mathcal{X}$ even is a set we say $\mathcal{C}$ is a **small** category, if $\mathcal{X}$ is a class but no set, we say that $\mathcal{C}$ is a **proper** category.

- $\mathcal{M}$ is a function of the form $\mathcal{M} : \mathcal{X}^2 \to \Omega$ that assigns every pair $(X, Y) \in \mathcal{X}^2$ of objects a set $\mathcal{M}(X, Y)$. The elements of $\mathcal{M}(X, Y)$ are called **morphisms** of $\mathcal{C}$ and we will also denote $\mathcal{C}(X, Y) := \mathcal{M}(X, Y)$. Lastly we will sometimes use the notation:

$$\mathrm{mor}(\mathcal{C}) \;:=\; \bigcup_{(X,Y)\in\mathcal{X}^2} \mathcal{M}(X, Y)$$

- For any triple $(X, Y, Z) \in \mathcal{X}^3$ of objects, there is a so-called **law of composition** $\circ_{X,Y,Z}$ of the morphisms. That is a map of the form

$$\mathcal{M}(X, Y) \times \mathcal{M}(Y, Z) \;\to\; \mathcal{M}(X, Z)$$

 If $\varphi \in \mathcal{M}(X, Y)$ and $\psi \in \mathcal{M}(Y, Z)$ are any morphisms of $\mathcal{C}$ we will write $\psi \circ \varphi$ as an abbreviation of $\circ_{X,Y,Z}(\varphi, \psi)$.

(C1) For any four objects U, X, Y and $Z \in \mathcal{X}$ and any morphisms $\varphi \in \mathcal{M}(U, X)$, $\psi \in \mathcal{M}(X, Y)$ and $\chi \in \mathcal{M}(Y, Z)$ we always have the following law of **associativity** of the composition

$$(\chi \circ \psi) \circ \varphi \;=\; \chi \circ (\psi \circ \varphi)$$

(C2) For any object $Y \in \mathcal{X}$ of $\mathcal{C}$ there is a morphism $\mathbb{1}_Y \in \mathcal{M}(Y, Y)$, called the **identity** on Y, that satisfies the following two properties:

$$\forall\, X \in \mathcal{X}\; \forall\, \varphi \in \mathcal{M}(X, Y) \;:\; \mathbb{1}_Y \circ \varphi \;=\; \varphi$$
$$\forall\, Z \in \mathcal{X}\; \forall\, \chi \in \mathcal{M}(Y, Z) \;:\; \chi \circ \mathbb{1}_Y \;=\; \chi$$

(11.2) Remark:
In any category $\mathcal{C}$, for any object $Y \in \mathrm{obj}(\mathcal{C})$ the identity morphism $\mathbb{1}_Y$ guaranteed by property (C2) already is uniquely determined.
Because if E_Y and $I_Y \in \mathcal{C}(Y, Y)$ both satisfy the properties of $\mathbb{1}_Y$ in (C2), then we could take $\varphi = I_Y$ and $\chi = E_Y$ to find $I_Y = \varphi = E_Y \circ \varphi = E_Y \circ I_Y$ and likewise $E_Y = \chi = \chi \circ I_Y = E_Y \circ I_Y$. Together this is $I_Y = E_Y \circ I_Y$ and $E_Y = E_Y \circ I_Y$ such that $E_Y = I_Y$.

(11.3) Remark:
In case of doubt let us append some comments on this: We can use almost any construction of sets for classes, too. If $\mathcal{X}$ and $\mathcal{Y}$ are classes and $X \in \mathcal{X}$ and $Y \in \mathcal{Y}$ are sets therein, then the ordered pair (X,Y) is a well-defined set again (namely $\{X,\{X,Y\}\}$). Therefore we can build up the *product* of the classes $\mathcal{X}$ and $\mathcal{Y}$, which is just another class

$$\mathcal{X} \times \mathcal{Y} \;:=\; \{\,(X,Y) \mid X \in \mathcal{X},\, Y \in \mathcal{Y}\,\}$$

A *relation* between $\mathcal{X}$ and $\mathcal{Y}$ is a subset (or more correctly a *subclass*) of $\mathcal{X} \times \mathcal{Y}$ and thereby a class in itself. A *function* $\mathcal{X} \to \mathcal{Y}$ is a relation between $\mathcal{X}$ and $\mathcal{Y}$ satisfying certain properties (totally defined and right-unique) and thereby a class again. This is how we can understand $\mathcal{M}$ as a class, that is a function from the product $\mathcal{X} \times \mathcal{X}$ to the universe Ω, in other words yet, a suitable subclass $\mathcal{M} \subseteq \mathcal{X} \times \mathcal{X} \times \Omega$. Even the law of composition $\circ$ is a function of the form $\circ : \mathcal{X}^3 \to \Omega$ in such a way that $\circ_{X,Y,Z} = \circ(X,Y,Z)$ is a function of the form

$$\circ_{X,Y,Z} \;\in\; \mathcal{F}\big(\mathcal{M}(X,Y) \times \mathcal{M}(Y,Z),\, \mathcal{M}(X,Z)\big)$$

As $\mathcal{M}(X,Y) \times \mathcal{M}(Y,Z)$ and $\mathcal{M}(X,Z)$ are sets there is a set of functions and $\circ_{X,Y,Z}$ is one of these – and hence $\circ_{X,Y,Z} \in \Omega$ a set again. So in fact all these constructions can be done with classes as well. There are some things to be aware of, however: As a function between classes $\mathcal{X} \to \mathcal{Y}$ is a class again, we *cannot* built up the class of all functions $\mathcal{F}(\mathcal{X},\mathcal{Y})$, as the elements need not be sets here! We will have to avoid this construction entirely.
In fact we cannot even build up an ordered pair $(\mathcal{X},\mathcal{Y})$ of classes, in the von Neumann way $\{\mathcal{X},\{\mathcal{X},\mathcal{Y}\}\}$, for the same reason: The elements need not be sets. But we only need to use this naively: That is two categories $\mathcal{C} = (\mathcal{X},\mathcal{M},\circ_{\mathcal{C}})$ and $\mathcal{D} = (\mathcal{Y},\mathcal{N},\circ_{\mathcal{D}})$ are considered *equal* $\mathcal{C} = \mathcal{D}$ if they share the same objects $\mathcal{X} = \mathcal{Y}$, for any two objects X, $Y \in \mathcal{X}$ they have the same morphisms $\mathcal{M}(X,Y) = \mathcal{N}(X,Y)$ and for any three objects X, Y, $Z \in \mathcal{X}$ and morphisms $\varphi \in \mathcal{M}(X,Y)$, $\psi \in \mathcal{M}(Y,Z)$ the respective compositions agree: $\psi \circ_{\mathcal{C}} \varphi = \psi \circ_{\mathcal{D}} \varphi$.

(11.4) Example:

(i) Our first example shall be the category **Set** of sets as this is where the terminology of categories comes from. The objects of this category simply are all the sets there are, that is $\mathrm{obj}(\mathbf{Set}) := \Omega$. Recall that the universe Ω is the class of all sets. Now for any two sets X and Y the morphisms of **Set** simply are all the functions from X to Y

$$\mathbf{Set}(X,Y) \;:=\; \mathcal{F}(X,Y)$$

Note that in case $X = \emptyset$ or $Y = \emptyset$ we also have $\mathcal{F}(X,Y) = \{\emptyset\}$, as $\emptyset$ is the only subset of $X \times Y$ and this trivially satisfies the properties of a function. The law of composition $\circ$ of **Set** is the usual composition of functions, that is if $f \in \mathbf{Set}(X,Y)$ and $g \in \mathbf{Set}(Y,Z)$ then $g \circ f \in \mathbf{Set}(X,Z)$ is the function defined by $g \circ f := gf$ which is $(g \circ f)(x) := g(f(x))$. The identity on the set Y is the identity map $\mathbb{1}_Y(y) = y$. In case $Y = \emptyset$ we have $\mathbb{1}_Y = \emptyset$ again.

($\diamondsuit$) Looking ahead we already note the following: In this category the epimorphisms are precisely the surjective maps, monomorphisms are precisely the injective maps and hence isomorphisms are precisely the bijective maps. The empty set $\emptyset$ is the one and only initial object of **Set**, whereas any set X with $\#X = 1$ is a terminal object.

(ii) As a next example let us introduce the category **Ring** of commutative rings. That is $\mathrm{obj}(\mathbf{Ring}) :=$ the class of all commutative rings $(R, +, \cdot)$. And for any two objects $\mathcal{R} = (R, +, \cdot)$ and $\mathcal{S} = (S, +, \cdot)$ the morphisms of **Ring** are just the usual homomorphisms of rings

$$\mathbf{Ring}(\mathcal{R}, \mathcal{S}) \;:=\; \mathrm{rhom}(R, S)$$

Note that $\mathcal{R}$ and $\mathcal{S}$ are triples of sets here and not classes, in contrast to our usual convention. Hence we will also write $\mathbf{Ring}(R, S)$ for the set of morphisms, as we did before, since the algebraic operations $+$ and $\cdot$ on R and S respectively, are understood. The law of composition $\circ$ of **Ring** is the usual composition of functions, that we used for **Set** already. And clearly $\mathbb{1}_R$ is an endomorphism of the ring $(R, +, \cdot)$ and hence we do have the identities required in (C2).

($\diamondsuit$) Looking ahead again we note: The notions of monomorphism, epimorphism and isomorphism in **Ring** coincide with the notions we introduced before. The zero-ring $R = 0$ is both, the initial and terminal object of **Ring**.

(iii) Another classic example is the category $\mathbf{Mod}_R$ of R-modules, over a fixed ring $(R, +, \cdot)$. That is $\mathrm{obj}(\mathbf{Mod}_R) :=$ the class of all modules $(M, +, \diamond)$ over the ring R and for any two R-modules $\mathcal{M} = (M, +, \diamond)$ and $\mathcal{N} = (N, +, \diamond)$ the morphisms are just the R-linear maps

$$\mathbf{Mod}_R(\mathcal{M}, \mathcal{N}) \;:=\; \mathrm{mhom}_R(M, N)$$

Again we will write $\mathbf{Mod}_R(M, N)$ in order to stay in conjunction with the notation used so far, which is not a problem, as the addition $+$ and scalar multiplication $\diamond$ on M and N are understood. The law of composition $\circ$ of $\mathbf{Mod}_R$ is the usual composition of functions, that we used for **Set** already. And clearly $\mathbb{1}_M$ is an endomorphism of the R-module $(M, +, \diamond)$ and hence we do have the identities required in (C2).

($\diamondsuit$) Looking ahead once more we note: The notions of monomorphism, epimorphism and isomorphism in $\mathbf{Mod}_R$ coincide with the notions we introduced before. The zero-module $M = 0$ is both, the initial and terminal object of $\mathbf{Mod}_R$.

(iv) If $(M, \circ)$ is a monoid with neutral element e, then this gives rise to a category $\mathcal{C}_M$ in the following way: $\mathcal{C}_M$ only has one object, say the set M itself: $\mathrm{obj}(\mathcal{C}_M) := \{M\}$. For the morphisms of $\mathcal{C}_M$ we just take the elements of M. As $\mathcal{C}_M$ has one object only, it suffices to define $\mathcal{C}_M(M, M) := M$. The composition of morphisms of $\mathcal{C}_M$ is the composition $\circ$ of elements of M. In particular the identity $\mathbb{1}_M = e$ is the neutral element of M.

And the converse is true, as well: If a category $\mathcal{C}$ has one object X only, then the morphisms $M := \mathcal{C}(X, X)$ form a monoid with $\mathbb{1}_X$ as neutral element under the composition $\circ$ of morphisms. And thereby $\mathcal{C}$ and $\mathcal{C}_M$ are much the same category, they only differ in the concrete object X or M they live on (this is to say: $(X \mapsto M,\ m \mapsto m)$ is an isofunctor).

(v) Another widely used category is that of topological spaces. Let us recall the definition of a **topological space** of section 6.1: This is an ordered pair $(X, \mathcal{T})$ consisting of a set X and a family of subsets $\mathcal{T} \subseteq \mathcal{P}(X)$. The sets $U \in \mathcal{T}$ are called the **open sets** of X and the collection $\mathcal{T}$ itself is said to be the **topology** on X. Hereby we demand, that $\emptyset$ and X are open sets and that finite intersections and arbitrary unions of open sets are open again. That is we require the following four properties of the topology $\mathcal{T}$:

(T1) $\emptyset \in \mathcal{T}$

(T2) $X \in \mathcal{T}$

(T3) $U, V \in \mathcal{T} \implies U \cap V \in \mathcal{T}$

(T4) $\mathcal{U} \subseteq \mathcal{T} \implies \bigcup \mathcal{U} \in \mathcal{T}$.

These are the objects of the category **Top** of topological spaces: Formally obj(**Top**) := the class of topological spaces $(X, \mathcal{T})$. If now $\mathcal{X} = (X, \mathcal{T}_X)$ and $\mathcal{Y} = (Y, \mathcal{T}_Y)$ are topological spaces then a function $f : X \to Y$ is said to be **continuous** if the preimage of an open set in Y is open in X, that is iff for any $V \in \mathcal{T}_Y$ we have $f^{-1}(V) \in \mathcal{T}_X$. The morphisms of **Top** are precisely the continuous functions in this sense

$$\mathbf{Top}(\mathcal{X}, \mathcal{Y}) \;:=\; \left\{ f : X \to Y \mid \forall\, V \in \mathcal{T}_Y \,:\, f^{-1}(V) \in \mathcal{T}_X \right\}$$

Hence we have $\mathbf{Top}(\mathcal{X}, \mathcal{Y}) \subseteq \mathcal{F}(X, Y)$ and can take the usual composition of maps, as in (i), as the law of composition $\circ$ for **Top**. Usually $\mathbf{Top}(\mathcal{X}, \mathcal{Y})$ is just denoted as $C(X, Y)$. Yet as this notation suppresses the topologies $\mathcal{T}_X$ and $\mathcal{T}_Y$ involved, it can only be used, when these are understood. Clearly $\mathbb{1}_Y^{-1}(V) = V$ such that the identity map on Y is continuous. As the associativity of $\circ$ is inherited from **Set** we find that **Top** indeed is a well-defined category.

($\diamondsuit$) Looking ahead, one more time, we find: The isomorphisms in **Top** are bijective, continuous maps. But as the inverse of a continuous map need not be continuous, this is not equivalent. The isomorphisms of this category are called **homeomorphisms** or **bicontinuous** maps. This is a bijective map $f \in C(X, Y)$ such that $f^{-1} \in C(Y, X)$ again. A counter-example is the following: Take $X_1 = X_2 = \{0, 1\}$ under the topologies $\mathcal{T}_1 := \mathcal{P}(X)$ and $\mathcal{T}_2 := \{\emptyset, X\}$. Then $\mathbb{1}_X : X_1 \to X_2$ is bijective and continuous, but its inverse $\mathbb{1}_X : X_2 \to X_1$ is not continuous.

(vi) Another neat application are **punctuated topological spaces**, these are triples $(X, \mathcal{T}, x_*)$ where $(X, \mathcal{T})$ is a topological space and $x_* \in X$ is a point. These are the objects of the category $\mathbf{Top}_*$ of punctuated topological spaces obj($\mathbf{Top}_*$) := the class of all punctuated topological spaces $(X, \mathcal{T}, x_*)$. A morphism f from $\mathcal{X} = (X, \mathcal{T}_X, x_*)$ to $(Y, \mathcal{T}_Y, y_*)$ is a continuous map, that respects the fixed point $f(x_*) = y_*$, that is

$$\mathbf{Top}_*(\mathcal{X}, \mathcal{Y}) \;:=\; \{ f \in \mathbf{Top}(\mathcal{X}, \mathcal{Y}) \mid f(x_*) = y_* \}$$

The law of composition $\circ$ once more is just the usual composition of maps and as $\mathbb{1}_Y(y_*) = y_*$ we also have the identity morphisms required for a category.

(vii) Let us return to our introductory example, the category of sets, and expand it a little: We want to introduce the category **Rel** of relations - though the name is not perfectly chosen, as it refers to the morphism not the objects. The objects are all the sets again, $\mathrm{obj}(\mathbf{Rel}) := \Omega$. But given any two sets X, Y the morphisms from X to Y are just the relations

$$\mathbf{Rel}(X,Y) \;:=\; \mathcal{P}\big(X \times Y\big)$$

If now $R \subseteq X \times Y$ and $S \subseteq Y \times Z$ are relations between X and Y resp. between Y and Z, then we define the composition of these $S \circ R = SR$ in the following way

$$SR \;:=\; \{\, (x,z) \in X \times Z \mid \exists\, y \in Y \,:\, (x,y) \in R \text{ and } (y,z) \in S \,\}$$

Note that in the usual notation this reads as: $xSRz$ if and only if xRy and ySz for some $y \in Y$. It is easy to see that this construction is associative and the identity $\mathbb{1}_Y$ on Y is given to be the diagonal (i.e. the identity function) $\mathbb{1}_Y = \{\, (y,y) \mid y \in Y \,\}$.

(viii) Our second last example will be a general construction: Given any category $\mathcal{C}$ we define the **opposite category** $\mathcal{C}^{\mathrm{op}}$ of $\mathcal{C}$ by keeping the objects, but reversing the direction of all morphisms. Formally $\mathcal{C}^{\mathrm{op}}$ is defined in the following way: The objects of $\mathcal{C}^{\mathrm{op}}$ are just the objects of $\mathcal{C}$ again

$$\mathrm{obj}\big(\mathcal{C}^{\mathrm{op}}\big) \;:=\; \mathrm{obj}(\mathcal{C})$$

Now for any two objects X, $Y \in \mathrm{obj}(\mathcal{C}^{\mathrm{op}})$ the morphisms from X to Y are just the morphisms of $\mathcal{C}$ from Y to X. Consequentially the law of composition of $\mathcal{C}^{\mathrm{op}}$ is just the law of composition of $\mathcal{C}$ reversed: If $f \in \mathcal{C}^{\mathrm{op}}(X,Y)$ and $g \in \mathcal{C}^{\mathrm{op}}(Y,Z)$ then

$$\mathcal{C}^{\mathrm{op}}(X,Y) \;:=\; \mathcal{C}(Y,X)$$

$$g \circ f \;:=\; f \circ_{\mathcal{C}} g \;\in\; \mathcal{C}^{\mathrm{op}}(X,Z)$$

Thereby the identity $\mathbb{1}_Y$ of $\mathcal{C}$ also is the identity on Y of $\mathcal{C}^{\mathrm{op}}$. ($\diamondsuit$) And looking ahead it is clear that monomorphisms and epimorphisms are interchanged by going from $\mathcal{C}$ to $\mathcal{C}^{\mathrm{op}}$. Isomorphisms are preserved, but initial and terminal objects are interchanged again.

(viii) ($\diamondsuit$) Our final example is a little more sophisticated - it is the underlying concept of differential and algebraic geometry - **spaces with** $\mathbb{F}$-valued **functions**, where $(\mathbb{F},+,\cdot)$ is a fixed field. Let us first define the objects of $\mathbf{Space}_{\mathbb{F}}$ this category: A space with functions is an ordered triple $(X,\mathcal{T},\mathcal{O})$ satisfying the following properties:

(S1) $(X,\mathcal{T})$ is a topological space.

(S2) $\mathcal{O}$ is a collection of $\mathbb{F}$-algebras $\mathcal{O}(U) \;\leq_{\mathrm{a}}\; \mathcal{F}(U,\mathbb{F})$ of $\mathbb{F}$-valued functions, where $U \in \mathcal{T}$ is an open subset of X. These are called the *regular functions* on X.

(S3) If U, $V \subseteq X$ are open subsets with $U \subseteq V$, then we require that for any regular function $s \in \mathcal{O}(V)$ the restriction $s\big|_U \in \mathcal{O}(U)$ is regular again.

(S4) If $U \subseteq X$ is open and $r \in \mathcal{O}(U)$ a regular function, then we require, that the non-zero locus $D(r) := \{\, x \in U \mid r(x) \neq 0 \,\} \subseteq X$ is open and that $1/r \in \mathcal{O}(D(r))$ is regular again.

(S5) If $\mathcal{U} \subseteq \mathcal{T}$ is a collection of open subsets of X and $V := \bigcup \mathcal{U} \subseteq X$ is their union, then for any $s \in \mathcal{F}(V, \mathbb{F})$ we require, that being regular is determined locally, in the sense that

$$\Big(\forall\, U \in \mathcal{U} \,:\, s\big|_U \in \mathcal{O}(U) \implies s \in \mathcal{O}(V) \Big)$$

Now consider two spaces with functions $(X, \mathcal{T}_X, \mathcal{O}_X)$ and $(Y, \mathcal{T}_Y, \mathcal{O}_Y)$ over the common field $\mathbb{F}$. Then a morphisms μ in this category is just a continuous map $\mu : X \to Y$ such that for any open subset $V \subseteq Y$ and any regular map $s \in \mathcal{O}_Y(V)$ the composition $s\mu : \mu^{-1}(V) \to \mathbb{F}$ is a regular map $s\mu \in \mathcal{O}_X(\mu^{-1}(V))$ again. Therefore a morphism $\mu : (X, \mathcal{T}_X, \mathcal{O}_X) \to (Y, \mathcal{T}_Y, \mathcal{O}_Y)$ always induces its *comorphism* $\mu^*(V)$ for every open subset $V \subseteq Y$, which is a homomorphism of $\mathbb{F}$-algebras

$$\mu^*(V) \;:\; \mathcal{O}_Y(V) \to \mathcal{O}_X(\mu^{-1}(V)) \;:\; s \mapsto s\mu$$

The composition of morphisms is the usual composition of functions, therefore associativity and the existence of an identity are granted. Altogether we have introduced another category $\mathbf{Space}_{\mathbb{F}}$, that encompasses affine varieties of algebraic geometry and manifolds of differential geometry.

(11.5) Example:
We can even model partially ordered sets in the language of category theory: Let $\mathcal{I}$ be any class and let $\leq$ have the properties of a partial order on $\mathcal{I}$. That is (1) $i \leq i$, (2) $i \leq j$ and $j \leq k$ implies $i \leq k$ and (3) $i \leq j$ and $j \leq i$ implies $i = j$ for any i, j and $k \in \mathcal{I}$. Then we define the corresponding **arrow category** $\mathcal{A}_\leq$ in the following way: The objects of $\mathcal{A}_\leq$ are $\mathrm{obj}(\mathcal{A}_\leq) := \mathcal{I}$. And for any two objects i, $j \in \mathcal{I}$ we define the sets of morphisms

$$\mathcal{A}_\leq(i,j) \;:=\; \begin{cases} \{0,1\} \text{ if } i \leq j \\ \{0\} \text{ if not} \end{cases}$$

That is $i \leq j$ is equivalent to $1 \in \mathcal{A}_\leq(i,j)$. This allows to reconstruct $\leq$ from its arrow category. The composition is quite simple, the morphisms are either 0 or $1 \in \mathbb{Z}$, then we define

$$\mathcal{A}_\leq(i,j) \times \mathcal{A}_\leq(j,k) \;\to\; \mathcal{A}_\leq(i,k) \;:\; (\alpha, \omega) \mapsto \alpha\omega$$

Clearly this is associative and turns $1 \in \mathcal{A}_\leq(i,i)$ into the identity $\mathbb{1}_i$. Nota this also is well-defined: We get $\alpha\omega = 1$ if and only if $\alpha = 1$ and $\omega = 1$. But this implies $i \leq j$ and $j \leq k$. Thus we have $i \leq k$ by transitivity and hence $1 \in \mathcal{A}_\leq(i,k)$. ($\diamondsuit$) Some authors like to install an order in a category $\mathcal{C}$ by prescribing a functor from an arrow-category to $\mathcal{C}$, but we see no benefit in this abstraction.

(11.6) Remark:
Most of the examples above have been *concrete categories*, meaning the objects are sets with some additional structure (e.g. X in a topological space $\mathcal{X} = (X, \mathcal{T})$), the morphisms $\mathcal{C}(\mathcal{X}, \mathcal{Y}) \subseteq \mathcal{F}(X, Y)$ are certain functions on the underlying sets (e.g. $f : X \to Y$ between the topological spaces $\mathcal{X} = (X, \mathcal{T}_X)$ and $\mathcal{Y} = (Y, \mathcal{T}_Y)$) and the law of composition $\circ$ is just the usual composition of functions. This is commonplace, but later on we will regard chain complexes as objects where the morphisms will not only be simple functions.

(11.7) Definition:
If $\mathcal{B}$ and $\mathcal{C}$ are categories, then $\mathcal{B}$ is said to be a **subcategory** of $\mathcal{C}$ - written as $\mathcal{B} \leq \mathcal{C}$ - iff we have the following three properties

(1) $\text{obj}(\mathcal{B}) \subseteq \text{obj}(\mathcal{C})$

(2) For any objects X, $Y \in \text{obj}(\mathcal{B})$ we have $\mathcal{B}(X,Y) \subseteq \mathcal{C}(X,Y)$. If we even have $\mathcal{B}(X,Y) = \mathcal{C}(X,Y)$, then $\mathcal{B}$ is said to be a **full** subcategory of $\mathcal{C}$.

(3) For any objects X, Y, $Z \in \text{obj}(\mathcal{B})$ and any morphisms $\varphi \in \mathcal{B}(X,Y)$ and $\psi \in \mathcal{B}(Y,Z)$ the laws of composition agree

$$\psi \circ_{\mathcal{B}} \varphi \quad = \quad \psi \circ_{\mathcal{C}} \varphi$$

(11.8) Remark:
It is clear, that we get a subcategory $\mathcal{B}$ of $\mathcal{C}$, if we begin with a subclass $\mathcal{X} \subseteq \text{obj}(\mathcal{C})$ and for any X, $Y \in \mathcal{X}$ take a subset $\mathcal{M}(X,Y) \subseteq \mathcal{C}(X,Y)$ such that (1) for any $Y \in \mathcal{X}$ we have $\mathbb{1}_Y \in \mathcal{M}(Y,Y)$ and (2) for any X, Y, $Z \in \mathcal{X}$ and any $\varphi \in \mathcal{M}(X,Y)$ and $\psi \in \mathcal{M}(Y,Z)$ we have $\psi \circ \varphi \in \mathcal{M}(X,Z)$. Then $\mathcal{B} = (\mathcal{X}, \mathcal{M}, \circ)$ is a subcategory of $\mathcal{C}$, where the law of composition $\circ$ is inherited by restriction from $\mathcal{C}$. Also it is clear, that the relation $\leq$ of being a subcategory has the properties of a partial order, that is (1) $\mathcal{C} \leq \mathcal{C}$, (2) $\mathcal{C} \leq \mathcal{D}$ and $\mathcal{D} \leq \mathcal{C}$ together imply $\mathcal{C} = \mathcal{D}$ and (3) $\mathcal{B} \leq \mathcal{C}$ and $\mathcal{C} \leq \mathcal{D}$ together imply $\mathcal{B} \leq \mathcal{C}$.

(11.9) Example:

- The category of finite sets is a full subcategory of the category **Set** of sets. Likewise we get a full subcategory **Dom** of integral domains of the category **Ring** of commutative rings. All we need to do is fix the objects $\text{obj}(\mathbf{Dom}) :=$ the class of commutative rings $(R, +, \cdot)$, that are integral domains. The morphisms are the ring-homomorphisms and the law of composition $\circ$ is the usual composition of maps, as in **Ring**.

- The category **Set** is a subcategory of **Rel** that share the same objects $\text{obj}(\mathbf{Set}) = \text{obj}(\mathbf{Rel})$, but in which **Set** has fewer morphisms, than **Rel**. So **Set** is far from being a full subcategory.

- A third example of this sort: A topological space $(X, \mathcal{T})$ is said to be a T_1-space, iff for any x, $y \in X$ with $x \neq y$ there are open sets U, $V \in \mathcal{T}$ such that $x \in U \setminus V$ and $y \in V \setminus U$. Let us define the full subcategory $\mathbf{Top}_1$ of **Top** by taking $\text{obj}(\mathbf{Top}_1) :=$ the class of all topological spaces $(X, \mathcal{T})$ that satisfy the T_1-property. The morphisms are the continuous functions again and the law of composition is the usual composition of maps, as in **Top**.

- The category $\mathbf{Top}_*$ of punctuated topological spaces is *not* a subcategory of the category **Top** of topological spaces, as the objects of $\mathbf{Top}_*$ differ from those of **Top** (they also contain a fixed point). Of course we can embed $\mathbf{Top}_*$ into **Top** by forgetting about the point, but this will require the notion of functors, that will be the topic of the next section. We will return to this.

(11.10) Definition: (viz. 1321)
Consider any category $\mathcal{C}$ and any two objects $X, Y \in \mathrm{obj}(\mathcal{C})$ therein. If now $\varphi \in \mathcal{C}(X,Y)$ is a morphism, then (inspired by the respective notions for rings, modules, etc.) we define the following notions:

(i) The morphism φ is said to be a **monomorphism**, iff for any object $T \in \mathrm{obj}(\mathcal{C})$ we find that the composition from the left $\varphi_* : \mathcal{C}(T,X) \hookrightarrow \mathcal{C}(T,Y) : \tau \mapsto \varphi \circ \tau$ is injective. That is for any two morphisms $\tau, \tau' \in \mathcal{C}(T,X)$ we have that $\varphi \circ \tau = \varphi \circ \tau'$ implies $\tau = \tau'$.

(ii) The morphism φ is said to be a **split-monomorphism**, iff φ admits a *left-inverse* $\overline{\varphi} \in \mathcal{C}(Y,X)$. And this is equivalent to saying that the composition with φ from the right always is surjectve:

(a) There is another morphism $\overline{\varphi} \in \mathcal{C}(Y,X)$ satisfying $\overline{\varphi} \circ \varphi = \mathbb{1}_X$

(b) For any object $T \in \mathrm{obj}(\mathcal{C})$ we find that $\varphi^* : \mathcal{C}(Y,T) \twoheadrightarrow \mathcal{C}(X,T) : \tau \mapsto \tau \circ \varphi$ is surjective

(iii) The morphism φ is said to be an **epimorphism**, iff for any object $T \in \mathrm{obj}(\mathcal{C})$ we find that the composition from the right $\varphi^* : \mathcal{C}(Y,T) \hookrightarrow \mathcal{C}(X,T) : \tau \mapsto \tau \circ \varphi$ is injective. That is for any two morphisms $\tau, \tau' \in \mathcal{C}(Y,T)$ we have that $\tau \circ \varphi = \tau' \circ \varphi$ implies $\tau = \tau'$.

(iv) The morphism φ is said to be a **split-epimorphism**, iff φ admits a *right-inverse* $\overline{\varphi} \in \mathcal{C}(Y,X)$. And this is equivalent to saying that the composition with φ from the left always is surjectve:

(a) There is another morphism $\overline{\varphi} \in \mathcal{C}(Y,X)$ satisfying $\varphi \circ \overline{\varphi} = \mathbb{1}_Y$

(b) For any object $T \in \mathrm{obj}(\mathcal{C})$ we find that $\varphi_* : \mathcal{C}(T,X) \twoheadrightarrow \mathcal{C}(T,Y) : \tau \mapsto \varphi \circ \tau$ is surjective

(v) The morphism φ is said to be an **isomorphism**, iff it satisfies one (and hence all) of the following six equivalent properties (and in this case $\psi = \psi_X = \psi_Y$)

(a) φ is both, a split-monomorphism and an epimorphism

(b) φ is both, a monomorphism and a split-epimorphism

(c) There are some $\psi_X, \psi_Y \in \mathcal{C}(Y,X)$ such that $\psi_X \circ \varphi = \mathbb{1}_X$ and $\varphi \circ \psi_Y = \mathbb{1}_Y$

(d) There is a uniquely determined $\psi \in \mathcal{C}(Y,X)$ such that $\psi \circ \varphi = \mathbb{1}_X$ and $\varphi \circ \psi = \mathbb{1}_Y$

(e) For any object $T \in \mathrm{obj}(\mathcal{C})$ we find that $\varphi^* : \mathcal{C}(Y,T) \to \mathcal{C}(X,T) : \tau \mapsto \tau \circ \varphi$ is bijective

(f) For any object $T \in \mathrm{obj}(\mathcal{C})$ we find that $\varphi_* : \mathcal{C}(T,X) \to \mathcal{C}(T,Y) : \tau \mapsto \varphi \circ \tau$ is bijective

The uniquely determined ψ in property (d) is then called the **inverse** of φ, written as $\varphi^{-1} := \psi$. And we say the objects X and Y are **isomorphic**, iff there is an isomorphism $\psi \in \mathcal{C}(X,Y)$. We denote this by writing

$$X \cong Y \quad :\Longleftrightarrow \quad \exists\, \varphi \in \mathcal{C}(X,Y) \,:\, (d)$$

(vi) A morphism $\varphi \in \mathcal{C}(X,Y)$ where $X = Y$ is said to be an **endomorphism** of $X \in \mathrm{obj}(\mathcal{C})$ and an endomorphism, that also is an isomorphism is said to be an **automorphism** of $X \in \mathrm{obj}(\mathcal{C})$.

(vii) A category $\mathcal{C}$ is said to be **faithful**, iff it is a concrete category (i.e. the sets of morphisms $\mathcal{C}(X,Y)$ are subsets of the set of functions from X to Y) and any bijective morphism already is an isomorphism.

(11.11) Proposition: (viz. 1322)
Let $\mathcal{C}$ is a category X, Y and $Z \in \mathrm{obj}(\mathcal{C})$ are objects and $\Phi \in \mathcal{C}(X,Y)$ and $\Psi \in \mathcal{C}(Y,Z)$ be isomorphisms, then $\Psi \circ \Phi \in \mathcal{C}(X,Z)$ is an isomorphism, as well with inverse

$$\big(\Psi \circ \Phi\big)^{-1} \;=\; \Phi^{-1} \circ \Psi^{-1}$$

Thereby the relation $\cong$ of isomorphy on the objects of $\mathcal{C}$ has the properties of an equivalence relation, that is for any X, Y and $Z \in \mathrm{obj}(\mathcal{C})$ we get

(1) $X \cong X$

(2) if $X \cong Y$ then $Y \cong X$, as well

(3) if $X \cong Y$ and $Y \cong Z$, then $X \cong Z$, as well

(11.12) Definition:
Let $\mathcal{C}$ be any category, then an object $U \in \mathrm{obj}(\mathcal{C})$ is said to be **universal** or **initial**, iff for any other object $X \in \mathrm{obj}(\mathcal{C})$ there is a uniquely determined morphism φ from U to X. Formally iff

$$\forall\ X \in \mathrm{obj}(\mathcal{C}) \;:\; \exists!\ \varphi \in \mathcal{C}(U,X)$$

The dual notion is the following: An object $T \in \mathrm{obj}(\mathcal{C})$ is said to be **final** or **terminal**, iff for any other object $X \in \mathrm{obj}(\mathcal{C})$ there is a uniquely determined morphism φ from X to T. Formally again

$$\forall\ X \in \mathrm{obj}(\mathcal{C}) \;:\; \exists!\ \varphi \in \mathcal{C}(X,T)$$

(11.13) Lemma: (viz. 1322)
If $\mathcal{C}$ is an arbitrary category, than any two universal objects U and $V \in \mathrm{obj}(\mathcal{C})$ are isomorphic $U \cong V$. Likewise any two terminal objects S and $T \in \mathrm{obj}(\mathcal{C})$ are isomorphic $S \cong T$.

(11.14) Proposition: (viz. 1322)
Let $\mathcal{C}$ be any category and fix any objects X, Y and $Z \in \mathrm{obj}(\mathcal{C})$. Also consider the morphisms $\varphi \in \mathcal{C}(X,Y)$ and $\psi \in \mathcal{C}(Y,Z)$. Then the monomorphisms and epimorphisms of $\mathcal{C}$ satisfy the following properties:

(i) If $\mathcal{C}$ is a concrete category (that is for any objects X, Y of $\mathcal{C}$ the morphisms $\varphi \in \mathcal{C}(X,Y)$ are functions $\varphi : X \to Y$ and the composition of morphisms is the usual composition of functions), then we get: If φ is an injective morphism, then φ is a monomorphism. And if φ is a surjective morphism, then φ is an epimorphism.

(ii) Any split-monomorphism already is a monomorphism. Likewise any split-epimorphism already is an epimorphism. (The converse need not be true, in general).

(iii) If both φ and ψ are monomorphisms. Then $\psi \circ \varphi \in \mathcal{C}(X,Z)$ is a momomorphism, as well. Conversely: If $\psi \circ \varphi$ is a monomorphisms, then φ has to be a monomorphism, too.

(iv) If both φ and ψ are epimorphisms. Then $\psi \circ \varphi \in \mathcal{C}(X,Z)$ is an epimorphism, as well. Conversely: If $\psi \circ \varphi$ is an epimorphisms, then ψ has to be an epimorphism, too.

(v) Monomorphisms to initial objects are isomorphisms, that is: If Y is an initial object of $\mathcal{C}$ and φ is a monomorphism, then φ already is an isomorphism.

(vi) Epimorphisms from terminal objects are isomorphisms, that is: If Y is a terminal object of $\mathcal{C}$ and ψ is an epimorphism, then ψ already is an isomorphism.

(11.15) Example: (viz. 1323)

(i) In the category **Set** of sets, for any function $f : X \to Y$, the following are equivalent: (a) f is injective, (b) f is a split-monomorphism and (c) f is a monomorphism. Likewise (a) f is surjective, (b) is a split-epimorphism and f is an epimorphism.

(ii) Let us regard the the category $\mathbf{Mod}_R$ of R-modules over a (not necessarily commutative) ring $(R, +, \cdot)$. In this category we find the following equivalences for any objects (i.e. R-modules) M and N and any R-module homomorphism $\varphi : M \to N$:

$$\begin{aligned} \varphi \text{ is a monomorphism} &\iff \varphi \text{ is an injective morphism} \\ \varphi \text{ is an epimorphism} &\iff \varphi \text{ is a surjective morphism} \\ \varphi \text{ is an isomorphism} &\iff \varphi \text{ is a bijective morphism} \end{aligned}$$

(iii) Let us regard the the category **Ring** of rings. In this category we find the following equivalences for any objects (i.e. rings) R and S and any homomorphism $\varphi : R \to S$ of rings:

$$\begin{aligned} \varphi \text{ is a monomorphism} &\iff \varphi \text{ is an injective morphism} \\ \varphi \text{ is an isomorphism} &\iff \varphi \text{ is a bijective morphism} \end{aligned}$$

And clearly any surjective homomorphism of rings is an epimorphism in **Ring**. Yet $\zeta : \mathbb{Z} \to \mathbb{Q}$ defined by $\zeta(k) = k/1$ is an example of an epimorphism in the category **Ring**, that is not a surjective map.

(iv) The equivalences for morphisms in (ii) also hold true in the category **Set** of sets and the category **Group** of groups. And the equivalences in (iii) also hold true in the category $\mathbf{Alg}_R$ of R-algebras over a commutative ring $(R, +, \cdot)$.

(11.16) Definition:
Consider any category $\mathcal{C}$ and some objects X, Y and $Z \in \mathrm{obj}(\mathcal{C})$. If now $\varphi \in \mathcal{C}(Y, Z)$ and $\psi \in \mathcal{C}(X, Z)$ are morphisms with the same target Z, then we say that ψ **factors through** φ, written as $\varphi \mid \psi$, iff

$$\varphi \mid \psi \quad :\iff \quad \exists\, \varphi' \in \mathcal{C}(X, Y) \,:\, \psi = \varphi \circ \varphi'$$

Now for any two morphisms $\psi_1 \in \mathcal{C}(X_1, Z)$ and $\psi_2 \in \mathcal{C}(X_2, Z)$ with the same target Z, but arbitrary domains X_1, $X_2 \in \mathrm{obj}(\mathcal{C})$, we define the relation of **bimorphism equivalence** by

$$\begin{aligned} \psi_1 \sim \psi_2 \quad &:\iff \quad \psi_1 \mid \psi_2 \text{ and } \psi_2 \mid \psi_1 \\ &\iff \quad \exists\, \psi_1' \in \mathcal{C}(X_2, X_1) \text{ and } \exists\, \psi_2' \in \mathcal{C}(X_1, X_2) \,:\, \psi_2 = \psi_1 \circ \psi_1' \text{ and } \psi_1 = \psi_2 \circ \psi_2' \end{aligned}$$

(11.17) Proposition: (viz. 1326)
If $\mathcal{C}$ is any category $Z \in \mathrm{obj}(\mathcal{C})$ is any object, then the bimorphism relation $\sim$ acts as an equivalence relation on the class of all morphisms of $\mathcal{C}$ with target Z. That is: Given any morphisms $\psi_k \in \mathcal{C}(X_k, Z)$ where $X_k \in \mathrm{obj}(\mathcal{C})$ and $k \in 1 \ldots 3$ we get the properties

(1) $\psi_1 \sim \psi_1$

(2) $\psi_1 \sim \psi_2 \implies \psi_2 \sim \psi_1$

(3) $\psi_1 \sim \psi_2$ and $\psi_2 \sim \psi_2 \implies \psi_1 \sim \psi_3$

Now suppose ψ_1 and ψ_2 are monomorphisms, with $\psi_1 \sim \psi_2$. Then the morphisms ψ_1' and ψ_2' satisfying $\psi_2 = \psi_1 \circ \psi_1'$ and $\psi_1 = \psi_2 \circ \psi_2'$ are uniquely determined and mutually inverse $\psi_2' = (\psi_1')^{-1}$.

(11.18) Definition:
Consider a category $\mathcal{C} = (\mathcal{X}, \mathcal{M}, \circ)$ such that for any pair of objects $X, Y \in \mathrm{obj}(\mathcal{C}) = \mathcal{X}$ the morphisms carry the structure of a commutative group

$$\mathcal{A}(X,Y) \;=\; \big(\mathcal{C}(X,Y), +\big)$$

Note that the operations $+$ actually depend on (X,Y), but by abuse of notation we denote all by the same symbol. Likewise we denote the neutral element of $\mathcal{C}(X,Y)$ by 0 instead of $0_{X,Y}$ though it also depends on (X,Y). Let $\mathcal{A}$ be the assignment $(X,Y) \mapsto \mathcal{A}(X,Y)$, then the triple $(\mathcal{X}, \mathcal{A}, \circ)$ is said to be an **additive category**, iff for any objects X, Y, $Z \in \mathrm{obj}(\mathcal{C})$ and any morphisms φ, φ_1, $\varphi_2 \in \mathcal{C}(X,Y)$ and ψ, ψ_1, $\psi_2 \in \mathcal{C}(Y,Z)$ we get

$$\begin{aligned} \big(\psi_1 + \psi_2\big) \circ \varphi &= \big(\psi_1 \circ \varphi\big) + \big(\psi_2 \circ \varphi\big) \\ \psi \circ \big(\varphi_1 + \varphi_2\big) &= \big(\psi \circ \varphi_1\big) + \big(\psi \circ \varphi_2\big) \end{aligned}$$

Being a little sloppy we usually say that in this case $\mathcal{C}$ is an additive category itself, if the operations $+$ on the morphisms $\mathcal{C}(X,Y)$ are understood. Also we introduce the convention that the law of composition $\circ$ binds stronger than the addition $+$, that is we would write $\psi_1 \circ \varphi + \psi_2 \circ \varphi$ as an abbreviation of $(\psi_1 \circ \varphi) + (\psi_2 \circ \varphi)$ and likewise $\psi \circ \varphi_1 + \psi \circ \varphi_2$ for $(\psi \circ \varphi_1) + (\psi \circ \varphi_2)$.

(11.19) Example:

- The most prominent examples of additive categories are **Ring** and $\mathbf{Mod}_R$. Of course the additions $+$ on the morphisms are point-wise

$$\big(\varphi + \psi\big)(x) \;=\; \varphi(x) + \psi(x)$$

- A truly new example is the following: Let $(R, +, \cdot)$ be a commutative ring, this gives rise to a small category $\mathcal{R}$ with one object only: $\mathrm{obj}(\mathcal{R}) := \{R\}$. The morphisms are the multiplication functions:

$$\mathcal{R}(R,R) \;:=\; \{\, \lambda_a : u \mapsto au \mid a \in R \,\}$$

Then it is clear that $\mathcal{R}(R,R)$ carries an additive structure under the point-wise addition $\lambda_a + \lambda_b : u \mapsto (a+b)u$. It is also clear that $\lambda_0 = 0$ is the neutral element of this group and that $\lambda_1 = \mathbb{1}_R$ is the identity. Thus $\mathcal{R}$ is an additive category.

(11.20) Proposition: (viz. 1327)
Let $\mathcal{C}$ be an additive category, X, Y, $Z \in \mathrm{obj}(\mathcal{C})$ be objects and $\varphi \in \mathcal{C}(X,Y)$, $\psi \in \mathcal{C}(Y,Z)$ be morphisms of $\mathcal{C}$. Then we get the following identities:

$$\begin{aligned} \psi \circ 0 &= 0 \\ 0 \circ \varphi &= 0 \\ \varphi \circ (-\varphi) &= -(\psi \circ \varphi) \\ (-\psi) \circ \varphi &= -(\psi \circ \varphi) \end{aligned}$$

(11.21) Remark: $(\diamondsuit)$

- As promised let us present three separate ways how to formalize classes: The most direct approach is to use a two-sorted language, one sort for sets and the other sort for classes. This idea was pursued by Bernays and also is the way in which we presented the NBG-axioms in section 0.6. We will write sets by straight latin letters X, Y, ... and classes by script letters $\mathcal{X}$, $\mathcal{Y}$, ... There are two *element of* relations, one between sets $x \in X$ and the other between sets and classes $X \in \mathcal{X}$. Yet there is *no element of* relation between classes themselves. That is $\mathcal{X} \in \mathcal{Y}$ is an *illegal expression*! Then the NBG-axioms provide a set of rules how to handle sets and classes.

- There also is another approach introduced by Gödel, refined by Mendelson, that uses a one-sorted language only: All variable symbols stand for classes, but we introduce a predicate M that says 'the class X is a set': $M(X) := \exists\, \mathcal{X}\, (X \in \mathcal{X})$. Thereby M comes from the german word *menge* for set. The negation thereof $P(X) := \forall\, \mathcal{X}\, \neg(X \in \mathcal{X})$ then is 'X is a proper class'. The formula 'For any set X we have $\varphi(X)$' of Bernays can then be translated into $\forall\, X\, (M(X) \implies \varphi(X))$ and likewise 'There is a set X with $\varphi(X)$' can be translated into $\exists\, X\, (M(X) \wedge \varphi(X))$'. Under this translation these two approaches yield the same results.

- The third approach is to say a class is an expression of the form $\mathcal{X} = \{\, X \mid \varphi(X) \,\}$, where φ is any formula in the language of sets. E.g. the universe then is $\Omega = \{\, X \mid X = X \,\}$. And if X_0 is a fixed set (a constant symbol in an extension of the language) then X_0 also is a class in the form $X_0 = \{\, X \mid X = X_0 \,\}$. This is what we recommend for a naive understanding, but be aware, that this is not a real answer, since it is not founded on formal logic.

11.2 Functors

In the previous section we have studied categories, in a manner of speaking, these are the objects of category theory. The reason why category has been developed is to study the interplay between different categories. This is where functors arise - in this sense, functors are the morphisms between categories. The most prominent functor is the spec-functor, that turns a commutative ring into a topological space. To study functors is to study the relations between categories.

(11.22) Definition:
Suppose $\mathcal{C}$ and $\mathcal{D}$ are categories, then the ordered pair $F = (F_o, F_m)$ is said to be a **covariant functor** from $\mathcal{C}$ to $\mathcal{D}$, written as $F : \mathcal{C} \to \mathcal{D}$, iff $F_o : \mathrm{obj}(\mathcal{C}) \to \mathrm{obj}(\mathcal{D})$ is a function (of classes). For ease of notation we write $F(X) := F_o(X) \in \mathrm{obj}(\mathcal{D})$ for any object $X \in \mathcal{C}$. Also F_m is a class of functions that assigns any two objects $X, Y \in \mathrm{obj}(\mathcal{C})$ a function of the form

$$F_m(X,Y) \ : \ \mathcal{C}(X,Y) \to \mathcal{D}(F(X),F(Y))$$

By slight abuse of notation we will write $F(\varphi) := F_m(X,Y)(\varphi) \in \mathcal{D}(F(X),F(Y))$ for any morphism $\varphi \in \mathcal{C}(X,Y)$. Thereby, for any objects $X, Y, Z \in \mathrm{obj}(\mathcal{C})$ and any morphisms $\varphi \in \mathcal{C}(X,Y)$ and $\psi \in \mathcal{C}(Y,Z)$ we require the following identity:

$$F\big(\psi \circ_{\mathcal{C}} \varphi\big) \ = \ F(\psi) \circ_{\mathcal{D}} F(\varphi)$$

A **contra-variant functor** from $\mathcal{C}$ to $\mathcal{D}$, also written as $F : \mathcal{C} \to \mathcal{D}$, is much the same: F_o is just the same, as in the covariant case above, but for any two objects $F_m(X,Y)$ is a function of the form

$$F_m(X,Y) \ : \ \mathcal{C}(X,Y) \to \mathcal{D}(F(Y),F(X))$$

such that for any objects $X, Y, Z \in \mathrm{obj}(\mathcal{C})$ and any morphisms $\varphi \in \mathcal{C}(X,Y)$ and $\psi \in \mathcal{C}(Y,Z)$ we require the following identity:

$$F\big(\psi \circ_{\mathcal{C}} \varphi\big) \ = \ F(\varphi) \circ_{\mathcal{D}} F(\psi)$$

If $\mathcal{C}$ and $\mathcal{D}$ even are additive categories, then a (co- or contra- variant) functor $F : \mathcal{C} \to \mathcal{D}$ is said to be **additive**, iff for any two objects $X, Y \in \mathrm{obj}(\mathcal{C})$ and any two morphisms $\varphi_1, \varphi_2 \in \mathcal{C}(X,Y)$ we get

$$F\big(\varphi_1 + \varphi_2\big) \ = \ F(\varphi_1) + F(\varphi_2)$$

(11.23) Remark:

- Clearly, the notion of a contra-variant functor $F : \mathcal{C} \to \mathcal{D}$ is nothing but a covariant functor $F : \mathcal{C} \to \mathcal{D}^{\mathrm{op}}$ to the opposite category of $\mathcal{D}$.
- If $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{C} \to \mathcal{E}$ are functors of any kind, then we may define the composition $GF : \mathcal{C} \to \mathcal{E}$ by $GF(X) := G(F(X))$ and $GF(\varphi) := G(F(\varphi))$. The composition GF thereby is a functor again - covariant, if F and G are of the same kind and contra-variant, if F and G are of different types.

- Any category $\mathcal{C}$ has its **identity functor** $\mathbb{1}_{\mathcal{C}} : \mathcal{C} \to \mathcal{C}$, which is defined in the obvious way: For any object $X \in \mathrm{obj}(\mathcal{C})$ we let $\mathbb{1}_{\mathcal{C}}(X) := X$ and likewise for any morphism $\varphi \in \mathcal{C}(X,Y)$ we let $\mathbb{1}_{\mathcal{C}}(\varphi) := \varphi$. Then we get $\mathbb{1}_{\mathcal{C}} E = E$ for any category $\mathcal{B}$ and any functor $E : \mathcal{B} \to \mathcal{C}$ and $F\mathbb{1}_{\mathcal{C}} = F$ for any category $\mathcal{D}$ and any functor $F : \mathcal{C} \to \mathcal{D}$.

- If $F : \mathcal{C} \to \mathcal{D}$ is an additive functor between additive categories, then it is clear that $F(0) = 0$ and $F(-\varphi) = -F(\varphi)$ and hence $F(\psi - \varphi) = F(\psi) - F(\varphi)$ for any morphisms $\varphi, \psi \in \mathrm{mor}(\mathcal{C})$.

 The first identity is true, since $F(0) = F(0+0) = F(0) + F(0)$ and subtracting $F(0)$ we find $0 = F(0)$. The second equation follows immediately, as $0 = F(0) = F(\varphi - \varphi) = F(\varphi) + F(-\varphi)$ and subtracting $F(\varphi)$ this is $-F(\varphi) = F(-\varphi)$.

(11.24) Example:

- Our first, trivial example of a functor is the so-called *forgetful functor*. This can be defined for any concrete category, but we want to do it exemplarily for the category **Top** of topological spaces here. In general the forgetful functor strips the additional structure of the objects, picking out the base set and takes the morphisms as the functions they are. In the case of **Top** it reads as

$$\begin{array}{rcl} \mathbf{Top} & \to & \mathbf{Set} \\ (X,\mathcal{T}) & \mapsto & X \\ f & \mapsto & f \end{array}$$

- Now if $(R,+,\cdot)$ is a fixed commutative ring and $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ is a fixed ideal of R, recall the definition of the sub-module $\mathfrak{a}M$ of M

$$\mathfrak{a}M \;:=\; \left\{ \sum_{i=1}^{n} a_i x_i \;\middle|\; 1 \leq n \in \mathbb{N},\ a_i \in \mathfrak{a},\ x_i \in M \right\}$$

 As we have seen in (3.40.(vi)) the quotient module $M/\mathfrak{a}M$ is a well-defined $(R/\mathfrak{a})$-module under the scalar multiplication $(a+\mathfrak{a})(x+\mathfrak{a}M) := (ax)+\mathfrak{a}M$. Also if $\varphi : M \to N$ is an R-linear map, then we obtain a well-defined, $(R/\mathfrak{a})$-linear map $\varphi/\mathfrak{a} : M/\mathfrak{a}M \to N/\mathfrak{a}N$ by letting $(\varphi/\mathfrak{a})(x+\mathfrak{a}M) := \varphi(x)+\mathfrak{a}N$, according to (3.40.(vii)). It is clear that the operation $/\mathfrak{a}$ respects the composition of functions and hence we have an additive, covariant functor, given by

$$\begin{array}{rcl} \mathbf{Mod}_R & \to & \mathbf{Mod}_{R/\mathfrak{a}} \\ M & \mapsto & M\big/_{\mathfrak{a}M} \\ \varphi & \mapsto & \varphi\big/_{\mathfrak{a}} \end{array}$$

- Likewise if $(R,+,\cdot)$ is a fixed commutative ring and $U \subseteq R$ is a fixed, multiplicatively closed subset of R, we have defined the commutative ring $U^{-1}R$ in (2.116) and the module $U^{-1}M$ in (3.121). And if $\varphi : M \to N$ is an R-linear map, then by (3.125.(ii)) we obtain an $U^{-1}R$-linear map $U^{-1}\varphi : U^{-1}M \to U^{-1}N$ by letting $U^{-1}\varphi(x/u) := \varphi(x)/u$. Again it is clear, that the operation U^{-1} respects the composition of functions and hence we have another additive, covariant functor

$$\begin{aligned} \mathbf{Mod}_R &\to \mathbf{Mod}_{U^{-1}R} \\ M &\mapsto U^{-1}M \\ \varphi &\mapsto U^{-1}\varphi \end{aligned}$$

- An almost famous example if the **tensor functor**: Fix a commutative ring $(R, +, \cdot)$ and an R-module U then we get a covariant functor, by

$$\begin{aligned} \mathbf{Mod}_R &\to \mathbf{Mod}_R \\ M &\mapsto M \otimes U \\ \varphi &\mapsto \varphi \otimes \mathbb{1}_U \end{aligned}$$

 The construction of $M \otimes U$ and $\varphi \otimes \mathbb{1}_U$ have been given, in section 3.13 - just recall that $\varphi \otimes \mathbb{1}_U$ is defined by $x \otimes u \mapsto \varphi(x) \otimes u$. This functor will be denoted by $\bullet \otimes U$, thereby $\varphi \otimes U$ is an abbreviation of $\varphi \otimes \mathbb{1}_U$ (which we try to avoid). Due to the isomorphism $M \otimes U \cong_{\mathrm{m}} U \otimes M$ there is no reason to study the functor $U \otimes \bullet$ separately.

- If $\mathcal{C}$ is any category and $A \in \mathrm{obj}(\mathcal{C})$ is any fixed object of $\mathcal{C}$, then we obtain a covariant functor H_A by assigning each object $Y \in \mathrm{obj}(\mathcal{C})$ the set of morphisms $\mathcal{C}(A, Y)$ and each morphism $\psi \in \mathcal{C}$ the map $H_A(\psi) : \mathcal{C}(A, X) \to \mathcal{C}(A, Y)$ defined by $H_A(\psi)(\varphi) := \psi \circ \varphi$.

$$\begin{aligned} \mathcal{C} &\to \mathbf{Set} \\ Y &\mapsto \mathcal{C}(A, Y) \\ \psi &\mapsto \big(\varphi \mapsto \psi \circ \varphi\big) \end{aligned}$$

 The functor H_A is called **covariant hom-functor** and we usually write $\mathcal{C}(A, \bullet)$, for it e.g. $\mathrm{mhom}(A, \bullet)$ in case of $\mathcal{C} = \mathbf{Mod}_R$. Then the notation $\mathcal{C}(A, X) = H_A(X)$ is straightforward and $\mathcal{C}(A, \psi) = H_A(\psi) : \varphi \mapsto \psi \circ \varphi$ stands to reason. In complete analogy, fixing an object $B \in \mathrm{obj}(\mathcal{C})$ we obtain the **contra-variant hom-functor** $\mathcal{C}(\bullet, B)$ by

$$\begin{aligned} \mathcal{C} &\to \mathbf{Set} \\ X &\mapsto \mathcal{C}(X, B) \\ \varphi &\mapsto \big(\psi \mapsto \psi \circ \varphi\big) \end{aligned}$$

- Our last example is the foundation of algebraic geometry: The **spectrum functor**, that assigns every commutative ring $(R, +, \cdot)$ its *spectrum*, that is its set of prime ideals

$$\mathrm{Spec}(R) \;=\; \{\, \mathfrak{p} \trianglelefteq_{\mathrm{i}} R \mid \forall\, a, b \in R : ab \in \mathfrak{p} \implies a \in \mathfrak{p} \text{ or } b \in \mathfrak{p} \,\}$$

 Recall the notation $\mathbb{V}(\mathfrak{a}) := \{\, \mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{a} \subseteq \mathfrak{p} \,\}$, these are taken to be the *closed* sets of $\mathrm{Spec}(R)$. That is we get a topology on $\mathrm{Spec}(R)$ (called the *Zariski-topology*) by letting

$$\mathcal{Z}_R \;:=\; \{\, \mathrm{Spec}(R) \setminus \mathbb{V}(\mathfrak{a}) \mid \mathfrak{a} \trianglelefteq_{\mathrm{i}} R \,\}$$

It is easy to see, that the closed points in this topology are precisely the maximal ideals of R. And as for a ring homomorphism $\varphi : R \to S$ we have that $\varphi^{-1}(\mathfrak{q}) \trianglelefteq_{\mathrm{i}} R$ is prime, for any prime ideal $\mathfrak{q} \trianglelefteq_{\mathrm{i}} S$. Thus we obtain a well-defined map $\mathrm{Spec}(\varphi) : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ defined, by $\mathrm{Spec}(\varphi)(\mathfrak{q}) := \varphi^{-1}(\mathfrak{q})$. And this even is continuous for the Zariski-topology, as $\varphi^{-1}(\mathbb{V}(\mathfrak{b})) = \mathbb{V}(\varphi^{-1}(\mathfrak{b}))$ Altogether we have a contra-variant functor, given by

$$\begin{array}{rcl} \textbf{Ring} & \to & \textbf{Top} \\ R & \mapsto & \big(\mathrm{Spec}(R),\, \mathcal{Z}_R\big) \\ \varphi & \mapsto & \big(\mathfrak{q} \mapsto \varphi^{-1}(\mathfrak{q})\big) \end{array}$$

(11.25) Definition:
Let $\mathcal{C}$ and $\mathcal{D}$ be any categories and $F : \mathcal{C} \to \mathcal{D}$ be a covariant functor. By definition, for any two objects $X, Y \in \mathrm{obj}(\mathcal{C})$, F induces a map of the following form

$$\mathcal{C}(X,Y) \to \mathcal{D}\big(F(X),F(Y)\big) \,:\, \varphi \mapsto F(\varphi)$$

In the case of a contra-variant functor, all we have to do is substitute the range of this map by $\mathcal{D}(F(Y),F(X))$. Now F is said to be **faithful**, iff for any $X, Y \in \mathrm{obj}(\mathcal{C})$ the above map $\varphi \mapsto F(\varphi)$ is injective. And F is said to be **full**, iff for any $X, Y \in \mathrm{obj}(\mathcal{C})$ this map $\varphi \mapsto F(\varphi)$ is surjective.
And we say that the functor F is **essentially surjective**, iff for any object $Y \in \mathrm{obj}(\mathcal{C})$ there is an object $X \in \mathrm{obj}(\mathcal{C})$ such that $Y \cong E(X)$ are isomorphic.

(11.26) Proposition: (viz. 1327)
Let $\mathcal{C}$ and $\mathcal{D}$ be any categories and $F : \mathcal{C} \to \mathcal{D}$ be a covariant functor. Consider any two objects X and $Y \in \mathrm{obj}(\mathcal{C})$, then we obtain the following statements

(i) If $\Phi \in \mathcal{C}(X,Y)$ is an isomorphism, then $F(\varphi) \in \mathcal{D}(F(X),F(Y))$ is an isomorphism, too. And its inverse is given to be $F(\Phi)^{-1} = F(\Phi^{-1})$.

(ii) If F is full and faithful and $\Theta \in \mathcal{D}(F(X),F(Y))$ is an isomorphism, then there is a (uniquely determined) isomorphism $\Phi \in \mathcal{C}(X,Y)$ such that $F(\Phi) = \Theta$.

(iii) If F is full and faithful such that $F(X) = F(Y)$, then the objects $X \cong Y$ are isomorphic.

(11.27) Definition:
Let $\mathcal{C}$ and $\mathcal{D}$ be any categories and let $F : \mathcal{C} \to \mathcal{D}$ be any functor (co- or contravariant). Then F is said to be an **isofunctor**, iff there is another functor $\overline{F} : \mathcal{D} \to \mathcal{C}$ such that $F\overline{F}$ is the identity on $\mathcal{D}$ and $\overline{F}F$ is the identity on $\mathcal{C}$. More formally, we require the following properties

(1) $\forall\, U \in \mathrm{obj}(\mathcal{C})$ we get $\overline{F}(F(U)) = U$

(2) $\forall\, X \in \mathrm{obj}(\mathcal{D})$ we get $F(\overline{F}(X)) = X$

(3) $\forall\, U, V\mathrm{obj}(\mathcal{C})$ and $\varphi \in \mathcal{C}(U,V)$ we get $\overline{F}(F(\varphi)) = \varphi$

(4) $\forall\, X, Y\mathrm{obj}(\mathcal{D})$ and $\psi \in \mathcal{D}(X,Y)$ we get $F(\overline{F}(\psi)) = \psi$

We say that $\mathcal{C}$ and $\mathcal{D}$ are **isomorphic**, iff there is an isofunctor $F : \mathcal{C} \to \mathcal{D}$ and we denote this by $F : \mathcal{C} \xrightarrow{\sim} \mathcal{D}$ or simply by $\mathcal{C} \cong \mathcal{D}$. Nota it is clear that $\cong$ thereby has the properties of an equivalence relation. That is (1) $\mathcal{C} \cong \mathcal{C}$, (2) $\mathcal{C} \cong \mathcal{D}$ implies $\mathcal{D} \cong \mathcal{C}$ and (3) $\mathcal{C} \cong \mathcal{D}$ and $\mathcal{D} \cong \mathcal{E}$ implies $\mathcal{C} \cong \mathcal{E}$.

(11.28) Definition:
Let $\mathcal{C}$ and $\mathcal{D}$ be any categories and let $F, G : \mathcal{C} \to \mathcal{D}$ be any two covariant functors. Then a collection $\eta = (\eta_X)$ where $X \in \mathrm{obj}(\mathcal{C})$ is said to be a **natural transformation** from F to G, iff we get

(1) $\forall\, X \in \mathrm{obj}(\mathcal{C})$ we find $\eta_X \in \mathcal{D}(F(X), G(X))$

(2) $\forall\, X, Y \in \mathrm{obj}(\mathcal{C}), \forall\, \varphi \in \mathcal{C}(X, Y)$ we find the commutativity of the diagram $\eta_Y F(\varphi) = G(\varphi)\eta_X$ where the left-downwards morphisms is η_X and the right-downwards morphism is η_Y

$$\begin{array}{ccc} F(X) & \xrightarrow{F(\varphi)} & F(Y) \\ \downarrow & & \downarrow \\ G(X) & \xrightarrow{G(\varphi)} & G(Y) \end{array}$$

In this case we write $\eta : F \rightrightarrows G$. We say that η is a **natural isomorphism** iff (3) for any object $X \in \mathrm{obj}(\mathcal{C})$ the morphism $\eta_X : F(X) \xrightarrow{\sim} D(X)$ even is an isomorphism. And in this case F and G are said to be **naturally isomorphic**, which we denote by $F \cong G$. It is obvious how to define natural transformations between contravariant functors: Property (1) remains unchanged and in the diagram of property (2) we just have to reverse the direction of the horizontal arrows, that is $\eta_X F(\varphi) = G(\varphi)\eta_Y$.

(11.29) Example:
The following example is artificial, but illustrates the workings of a natural transformation: We regard the category **Set** of sets and define the functor $F : \mathbf{Set} \to \mathbf{Set}$ by $F(X) := X \times X$ for any set X and $F(f) : (x_1, x_2) \to (f(x_1), f(x_2))$ for any function $f : X \to Y$. The functor $G : \mathbf{Set} \to \mathbf{Set}$ is just the identity $G(X) := X$ and $G(f) := f$. Then $\eta = (\eta_X)$ is a natural transformation $\eta : F \rightrightarrows G$, where we define $\eta_X : X \times X \to X : (x_1, x_2) \mapsto x_1$.

(11.30) Definition:
Let $\mathcal{C}$ and $\mathcal{D}$ be any categories, then the pair $(E, \overline{E})$ is said to be an **equivalence** of the categories $\mathcal{C}$ and $\mathcal{D}$, iff we get the following properties (1) to (4). And in this case we write $(E, \overline{E}) : \mathcal{C} \sim \mathcal{D}$.

(1) $E : \mathcal{C} \to \mathcal{D}$ is a functor

(2) $\overline{E} : \mathcal{D} \to \mathcal{C}$ is a functor

(3) There is a collection (Φ_X) where $X \in \mathrm{obj}(\mathcal{C})$, such that any $\Phi(X) : X \to \overline{E}(E(X))$ is an isomorphism of $\mathcal{C}$ such that for any two objects X, $X' \in \mathrm{obj}(\mathcal{C})$ and any morphism $\varphi \in \mathcal{C}(X, X')$ we get the commutativity of the diagram $\Phi_{X'} \circ \varphi = \overline{E}(E(\varphi)) \circ \Phi_X$. That is the following diagram, where the left-downwards morphisms is Φ_X and the right-downwards morphism is $\Phi_{X'}$:

$$\begin{array}{ccc} X & \xrightarrow{\varphi} & X' \\ \downarrow & & \downarrow \\ \overline{E}(E(X)) & \xrightarrow{\overline{E}(E(\varphi))} & \overline{E}(E(X')) \end{array}$$

(4) There is a collection (Θ_Y) where $Y \in \mathrm{obj}(\mathcal{D})$, such that any $\Theta_Y : Y \to E(\overline{E}(Y))$ is an isomorphism of $\mathcal{D}$ such that for any two objects Y, $Y' \in \mathrm{obj}(\mathcal{D})$ and any morphism $\psi \in \mathcal{D}(Y, Y')$ we get the commutativity of the diagram $\Theta_{Y'} \circ \psi = E(\overline{E}(\psi)) \circ \Theta_Y$. That is the following diagram, where the left-downwards morphisms is Θ_Y and the right-downwards morphism is $\Theta_{Y'}$:

$$\begin{array}{ccc} Y & \xrightarrow{\psi} & Y' \\ \downarrow & & \downarrow \\ E(\overline{E}(Y)) & \xrightarrow{E(\overline{E}(\psi))} & E(\overline{E}(Y')) \end{array}$$

(11.31) Proposition: (viz. 1327)

(i) Equivalence of categories has the properties of an equivalence relation. That is for any categories $\mathcal{B}$, $\mathcal{C}$ and $\mathcal{D}$ we have the following properties: (1) $(\mathbb{1}, \mathbb{1}) : \mathcal{C} \sim \mathcal{C}$ under the identity functor $\mathbb{1}(X) := X$ and $\mathbb{1}(\varphi) := \varphi$. (2) If $(E, \overline{E}) : \mathcal{C} \sim \mathcal{D}$ is an equivalence of categories, then $(\overline{E}, E) : \mathcal{D} \sim \mathcal{C}$ is an equivalence of categories, as well. And (3) if $(D, \overline{D}) : \mathcal{B} \sim \mathcal{C}$ and $(E, \overline{E}) : \mathcal{C} \sim \mathcal{D}$ are equivalences of categories, then $(ED, \overline{DE}) : \mathcal{B} \sim \mathcal{D}$ is an equivalence of categories, again.

(ii) If $(E, \overline{E}) : \mathcal{C} \sim \mathcal{D}$ is an equivalence of the categories $\mathcal{C}$ and $\mathcal{D}$, then both, E and $\overline{E}$ are have all of the properties: They are full, faithful and essentially surjective.

(iii) If $E : \mathcal{C} \to \mathcal{D}$ is a (covariant) full, faithful and essentially surjective functor from the category $\mathcal{C}$ to the category $\mathcal{D}$, then E admits a *quasi-inverse* $\overline{E} : \mathcal{D} \to \mathcal{C}$, such that $(E, \overline{E}) : \mathcal{C} \sim \mathcal{D}$ is an equivalence of categories. A construction of $\overline{E}$ is given in the proof.

(iv) Let $\mathcal{C}$ and $\mathcal{D}$ be any categories and $E : \mathcal{C} \to \mathcal{D}$ and $\overline{E} : \mathcal{D} \to \mathcal{C}$ be covariant functors. Then the following statements are equivalent

 (a) $(E, \overline{E}) : \mathcal{C} \sim \mathcal{D}$ is an equivalence of categories

 (b) The compositions $E\overline{E}$ and $E\overline{E}$ are naturally isomorphic to the respective identity functors: That is we have $E\overline{E} \cong \mathbb{1}_{\mathcal{D}}$ and $\overline{E}E \cong \mathbb{1}_{\mathcal{C}}$.

categories: $\mathbf{C}_S$, $\mathbf{C}^\bullet$, $\mathbf{Bun}_\bullet$,
representable functors, Yoneda's lemma

11.3 Universal Properties

Categories are a very general concept. It's objects don't even have to be sets, like for example topological spaces, that consist of a base set X and a topology $\mathcal{T}$ on X. The cartesian product, for example, is a widely construction, that spawned direct products and direct sums. As is this construction can only be applied to sets. So how can we transfer this concept to general objects of a category?
The answer lies in studying the structure the cartesian product provides: It comes with projections from the product to the base sets, composing it. So in category theory we no longer use constructions of these objects, but rather fix how this new object interacts with others. If these properties are rigorous enough, the new object, e.g. the product, will be uniquely determined - up to isomorphism. Such a definition of an object by its properties is called a *universal property*.
The drawback is: By prescribing a universal property, it is neither clear, whether such an object exists, nor is it determined uniquely. We can only say, that any two objects satisfying a certain universal property are isomorphic. The existence can only be shown using a suitable construction, in the category given. The advantage is, that we get a unified treatment of like constructions (such as products) across very different categories. Let us start with the concept of products:

(11.32) Definition:
Consider any category $\mathcal{C}$, a non-empty index set I and for any $i \in I$ let $X_i \in \mathrm{obj}(\mathcal{C})$ be an object of $\mathcal{C}$. Then the (P, π_i) is said to be a **product** of the X_i, iff it satisfies the following three properties

(1) $P \in \mathrm{obj}(\mathcal{C})$ is an object of $\mathcal{C}$

(2) For any $i \in I$ we have $\pi_i \in \mathcal{C}(P, X_i)$, a morphism of $\mathcal{C}$

(3) For any other pair (U, φ_i), such that $U \in \mathrm{obj}(\mathcal{C})$ and $\varphi_i \in \mathcal{C}(U, X_i)$ there is a uniquely determined morphism $\varphi \in \mathcal{C}(U, P)$ such that (for any $i \in I$) the following diagrams commutes: $\varphi_i = \pi_i \circ \varphi$.

We continue with the objects X_i above. We likewise say, that (S, ε_i) is a **coproduct** (also called **direct sum**) of the X_i, iff it satisfies the following three, mirrored properties:

(1) $S \in \mathrm{obj}(\mathcal{C})$ is an object of $\mathcal{C}$

(2) For any $i \in I$ we have $E_i \in \mathcal{C}(X_i, S)$, a morphism of $\mathcal{C}$

(3) For any other pair (Y, φ_i), such that $Y \in \mathrm{obj}(\mathcal{C})$ and $\varphi_i \in \mathcal{C}(X_i, Y)$ there is a uniquely determined morphism $\varphi \in \mathcal{C}(S, Y)$ such that (for any $i \in I$) the following diagrams commutes: $\varphi_i = \varphi \circ \varepsilon_i$.

We say that the category $\mathcal{C}$ **admits products**, iff for any index-set I and any family (X_i) of objects, there is a product (P, π_i) of these X_i. Likewise we say that the category $\mathcal{C}$ **admits coproducts**, iff for any index-set I and any family (X_i) of objects, there is a product (S, ε_i) of these X_i.

(11.33) Proposition: (viz. 1330)

(i) Let $\mathcal{C}$ be a category and I a non-empty index set. For any $i \in I$ let $X_i \in \mathrm{obj}(\mathcal{C})$ be an object of $\mathcal{C}$. If both (P, π_i) and (P', π_i') are products of the X_i, then $P \cong P'$ are isomorphic. And thereby this isomorphism $\Phi : P \xrightarrow{\sim} P'$ is the one and only morphism $\Phi \in \mathcal{C}(P, P')$ that satisfies $\pi_i = \pi_i' \circ \Phi$ for any $i \in I$.

(ii) Let $\mathcal{C}$ be a category and I a non-empty index set. For any $i \in I$ let $X_i \in \mathrm{obj}(\mathcal{C})$ be an object of $\mathcal{C}$. If both (S, ε_i) and (S', ε'_i) are coproducts of the X_i, then $S \cong S'$ are isomorphic. And thereby this isomorphism $\Phi : S \xrightarrow{\sim} S'$ is the one and only morphism $\Phi \in \mathcal{C}(S, S')$ that satisfies $\varepsilon'_i = \Phi \circ \varepsilon_i$ for any $i \in I$.

(iii) Products (and coproducts) are preserved under equivalence of categories. Formally this is to say: Let $(E, \overline{E}) : \mathcal{C} \sim \mathcal{D}$ be an equivalence of the categories $\mathcal{C}$ and $\mathcal{D}$. Consider a family of objects $X_i \in \mathrm{obj}(\mathcal{C})$ where $i \in I \neq \emptyset$. Also let $P \in \mathrm{obj}(\mathcal{C})$ and for any $i \in I$ some $\pi_i \in \mathcal{C}(P, X_i)$. Then the following statements are equivalent

(a) (P, π_i) is a (co)product of the X_i

(b) $(E(P), E(\pi_i))$ is a (co)product of the $E(X_i)$

(11.34) Example:

(i) The category **Set** of sets admits products: If I is any non-empty set and for any $i \in I$ we are given an arbitrary set X_i then a product (P, π_i) of the X_i is given by the cartesian product

$$P \;:=\; \prod_{i \in I} X_i \;=\; \{\, (x_i) \mid \forall\, i \in I : x_i \in X_i \,\}$$

under the canonical projections $\pi_j : P \twoheadrightarrow X_j : (x_i) \mapsto x_j$. In fact, if U is any other set and for any $i \in I$ we are given some map $\varphi_i : U \to X_i$, then we can define $\varphi : U \to P$, by $\varphi(u) := (\varphi_i(u))$.

(ii) The category **Set** of sets also admits coproducts: If I is any non-empty set and for any $i \in I$ we are given an arbitrary set X_i then a coproduct (S, ε_i) of the X_i is given by the disjoint union

$$S \;:=\; \bigsqcup_{i \in I} X_i \;=\; \{\, (i, x_i) \mid \forall\, i \in I : x_i \in X_i \,\}$$

under the canonical embeddings $\varepsilon_j : X_j \hookrightarrow S : x_j \mapsto (j, x_j)$. In fact, if Y is any other set and for any $i \in I$ we are given some map $\varphi_i : X_i \to S$, then we can define $\varphi : S \to Y$, by $\varphi(i, x_i) := \varphi_i(x_i)$.

(iii) Fix any ring $(R, +, \cdot)$, then the category $\mathbf{Mod}_R$ of R-modules admits products: Let I be any non-empty set and for any $i \in I$ consider an R-module M_i. The direct product P of the M_i is the cartesian product of the M_i under the component-wise operations, as in (3.29). Then (P, π_i) is a product of the M_i, where $\pi_j : P \twoheadrightarrow M_j : (x_i) \mapsto x_j$ are the canonical projections, again. In fact, if U is any other R-module and for any $i \in I$ we are given an R-linear map $\varphi_i : U \to M_i$ then we can define $\varphi : U \to P$ by $\varphi(u) := \big(\varphi_i(u)\big)$.

(iv) The category $\mathbf{Mod}_R$ of R-modules over the ring R also admits coproducts: Let I be any non-empty set and for any $i \in I$ consider an R-module M_i. Then we take to the direct sum S of the M_i

$$S \;:=\; \bigoplus_{i \in I} M_i$$

and for any $j \in I$ we let $\iota_j : M_j \to S$ by $\iota_j(x_j) := (\overline{x}_i)$ where $\overline{x}_j := x_j$ and $\overline{x}_i := 0_i$ for any $i \in I$ with $i \neq j$. Then (S, ε_i) is a coproduct of the M_i. In fact, if N is any other R-module and for any $i \in I$ we are given an R-linear map $\varphi_i : M_i \to N$, then we can define $\varphi : S \to N$ by $\varphi : (x_i) \mapsto \big(\varphi_i(x_i)\big)$.

(v) The category **Ring** of rings admits products: Let I be any non-empty set and for any $i \in I$ consider a ring $(R_i, +, \cdot)$. The direct product P of the R_i is the cartesian product of the R_i under the componentwise operations, as in (1.94). Then (P, π_i) is a product of the R_i, where $\pi_j : P \twoheadrightarrow R_j : (a_i) \mapsto a_j$ are the canonical projections, again. In fact, if $(U, +, \cdot)$ is any other ring and for any $i \in I$ we are given a ring-homomorphism $\varphi_i : U \to R_i$ then we can define $\varphi : U \to P$ by $\varphi(u) := \big(\varphi_i(u)\big)$.

Coproducts are problematic: There is no obvious way how to define the canonical embeddings $\varepsilon_i : R_i \to S$. If we use the same maps, as in (iv), then the ε_i do not map 1_i to 1_S, even if I is finite. In case of commutative rings we can regard the R_i as $\mathbb{Z}$-algebras. And thereby we find a coproduct in form of the tensor product. This is the next item:

(vi) Fix any ring $(R, +, \cdot)$, then the category $\mathbf{cAlg}_R$ of commutative R-algebras admits *finite* coproducts: That is to say, if A_1 to A_n are commutative R-algebras, then we take to their tensor product, which is a commutative R-algebra, again

$$S \;:=\; A_1 \otimes \ldots \otimes A_n$$

Recall (3.145), there we defined the maps $\varepsilon_j : A_j \to S$, by taking $\varepsilon_1(x_1) := x_1 \otimes 1_2 \otimes \ldots \otimes 1_n$ up to $\varepsilon_n(x_n) := 1_1 \otimes \ldots \otimes 1_{n-1} \otimes x_n$. We have seen there, that these are R-algebra-homomorphisms, that make (S, ε_i) a product in the sense of category theory.

(vii) The category **Top** of topological spaces admits products: If I is any non-empty set and for any $i \in I$ we are given a topological space $(X_i, \mathcal{T}_i)$ then a product $\big((P, \mathcal{T}), \pi_i\big)$ of these is given by the cartesian product P under the product topology, defined in (6.14).

The π_j are the canonical projections $\pi_j : P \twoheadrightarrow X_j : (x_i) \mapsto x_j$ again. It has been shown in (6.29.(xi)), that the map φ in (i) is a morphism again. And therefore this construction truly satisfies the universal property of a product in the sense of category theory.

(11.35) Definition:
Fix any category $\mathcal{C}$ and a partially ordered set $(I, \leq)$. We say that (M_i, μ_i^j) is a **directed system** over I in $\mathcal{C}$, iff the following four properties are satisfied

(1) $\forall\, i \in I$ we get: $M_i \in \mathrm{obj}(\mathcal{C})$ is an object

(2) $\forall\, i, j \in I$ with $i \leq j$ we get: $\mu_i^j \in \mathcal{C}(M_i, M_j)$ is a morphism

(3) $\forall\, i \in I$ we get: $\mu_i^i = \mathbb{1}_{M_i}$ is the identity on M_i

(4) $\forall\, i, j$ and $k \in I$ with $i \leq j$ and $j \leq k$ we get: $\mu_j^k \circ \mu_i^j = \mu_i^k$

In this case the morphisms μ_i^j are said to be the **transition morphisms** of the directed system (M_i, μ_i^j). And (T, τ_i) is said to be a **direct target** of the directed system (M_i, μ_i^j), iff it satisfies the properties

(1) $T \in \mathrm{obj}(\mathcal{C})$ is an object

(2) $\forall\, i \in I$ we get: $\tau_i \in \mathcal{C}(M_i, T)$ is a morphism

(3) $\forall\, i, j \in I$ with $i \leq j$ we get: $\tau_i = \tau_j \circ \mu_i^j$

In this case the morphisms τ_i are said to be the **structural morphisms** of the direct target (T, τ_i). And finally (L, λ_i) is said to be an **direct limit** (or simply a **colimit**) of the directed system (M_i, μ_i^j), iff it is a direct target of (M_i, μ_i^j), that additionally satisfies the following *universal property*:

(4) For any direct target (T, τ_i) of (M_i, μ_i^j) there is a uniquely determined morphism $\tau \in \mathcal{C}(L, T)$ that satisfies the commutativity $\tau_i = \tau \circ \lambda_i$ for any $i \in I$.

(11.36) Definition:
Fix any category $\mathcal{C}$ and a partially ordered set $(I, \leq)$. We say that (M_i, μ_j^i) is an **inverse system** over I in $\mathcal{C}$, iff the following four properties are satisfied

(1) $\forall\, i \in I$ we get: $M_i \in \mathrm{obj}(\mathcal{C})$ is an object

(2) $\forall\, i, j \in I$ with $i \leq j$ we get: $\mu_j^i \in \mathcal{C}(M_j, M_i)$ is a morphism

(3) $\forall\, i \in I$ we get: $\mu_i^i = \mathbb{1}_{M_i}$ is the identity on M_i

(4) $\forall\, i, j$ and $k \in I$ with $i \leq j$ and $j \leq k$ we get: $\mu_j^i \circ \mu_k^j = \mu_k^i$

In this case the morphisms μ_j^i are said to be the **transition morphisms** of the inverse system (M_i, μ_j^i). And (T, τ_i) is said to be an **inverse target** of the inverse system (M_i, μ_j^i), iff it satisfies the properties

(1) $T \in \mathrm{obj}(\mathcal{C})$ is an object

(2) $\forall\, i \in I$ we get: $\tau_i \in \mathcal{C}(T, M_i)$ is a morphism

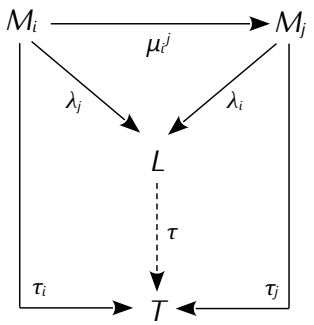
(3) $\forall\, i, j \in I$ with $i \leq j$ we get: $\tau_i = \mu_j^i \circ \tau_j$

In this case the morphisms τ_i are said to be the **canonical projections** of the inverse target (T, τ_i). And finally (L, λ_i) is said to be an **inverse limit** (or simply a **limit**) of the inverse system (M_i, μ_j^i), iff it is an inverse target of (M_i, μ_j^i), that additionally satisfies the following *universal property*:

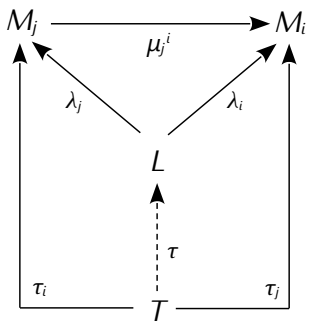
(4) For any inverse target (T, τ_i) of (M_i, μ_j^i) there is a uniquely determined morphism $\tau \in \mathcal{C}(T, L)$ that satisfies the commutativity $\tau_i = \lambda_i \circ \tau$ for any $i \in I$.

(11.37) Remark:
We have studies direct and inverse limits in the category of sets, topological spaces, rings, modules and algebras over a fixed commutative ring R in section 3.14 already. There we have used a constructive approach to find the direct resp. inverse limit. In the general context of category theory we may only rely on on the universal property to define these (up to isomorphism). So let us rewrite the diagrams involved in the definition in terms of the variable symbols used here:

universal property of the direct limit



universal property of the inverse limit



(11.38) Proposition: (viz. 1331)

(i) Let $\mathcal{C}$ be a category and $(I, \leq)$ be a partially ordered set and fix a directed system (M_i, μ_i^j) over I in $\mathcal{C}$. Now, if both (L, λ_i) and (L', λ_i') are direct limits of (M_i, μ_i^j), then $L \cong L'$ are isomorphic. And thereby this isomorphism $\Phi : L \xrightarrow{\sim} L'$ is the one and only morphism $\Phi \in \mathcal{C}(L, L')$ that satisfies $\lambda_i' = \Phi \circ \lambda_i$ for any $i \in I$.

(ii) Let $\mathcal{C}$ be a category and $(I, \leq)$ be a partially ordered set and fix an inverse system (M_i, μ_j^i) over I in $\mathcal{C}$. Now, if both (L, λ_i) and (L', λ_i') are inverse limits of (M_i, μ_j^i), then $L \cong L'$ are isomorphic. And thereby this isomorphism $\Phi : L \xrightarrow{\sim} L'$ is the one and only morphism $\Phi \in \mathcal{C}(L, L')$ that satisfies $\lambda_i = \lambda_i' \circ \Phi$ for any $i \in I$.

(iii) Direct and inverse limits are preserved under equivalence of categories. Formally this is to say: Let $(E, \overline{E}) : \mathcal{C} \sim \mathcal{D}$ be an equivalence of the categories $\mathcal{C}$ and $\mathcal{D}$. Let $(I, \leq)$ be a partially ordered set and (M_i, μ_i^j) be a directed system over I in $\mathcal{C}$. Also let (L, λ_i) be a direct target of (M_i, μ_i^j). Then the following statements are equivalent

 (a) (L, λ_i) is a direct limit of (M_i, μ_i^j)

 (b) $(E(L), E(\lambda_i))$ is a direct limit of $(E(M_i), E(\mu_i^j))$

 Likewise if (M_i, μ_j^i) is an inverse system over I in $\mathcal{C}$ and (L, λ_i) is an inverse target of (M_i, μ_j^i) then the following statements are equivalent

 (a) (L, λ_i) is an inverse limit of (M_i, μ_j^i)

 (b) $(E(L), E(\lambda_i))$ is an inverse limit of $(E(M_i), E(\mu_j^i))$

example: fibered product = pullback = special case of indirect limit (Wiki)
injective and projective objects

11.4 Abelian Categories

additive categories and their properties, additive functors, examples, kernel, cokernel and their properties, examples, canonical decomposition of morphisms, definition of abelian categories, left/right-exactness, examples: $\bullet/\mathfrak{a}$, $U^{-1}\bullet$, $\hom(,)$

Chapter 12

Valuations

siehe Bourbaki (commutative algebra) VI, mein Skriptum

Chapter 13

Symbols

Symbol	Content	Introduced in
$\mathbb{N}$	natural numbers $\{0,1,2,\dots\}$	-
$\mathbb{Z}$	integers = integer numbers	-
$\mathbb{Q}$	rational numbers = fractions of integers	(1.31)
$\mathbb{R}$	reals = real numbers	(1.27)
$\mathbb{R}^+$	positive reals $= \{ x \in \mathbb{R} \mid x \geq 0 \}$	-
$\mathbb{R}^-$	negative reals $= \{ x \in \mathbb{R} \mid x \leq 0 \}$	-
$\mathbb{R}_{>0}$	strictly positive reals $= \{ x \in \mathbb{R} \mid x > 0 \}$	-
$\mathbb{R}_{<0}$	strictly negative reals $= \{ x \in \mathbb{R} \mid x < 0 \}$	-
$\mathbb{C}$	complex numbers	(1.35)
$\mathbb{H}$	quaternions	(1.38)
$\overline{z}$	$= a - ib$ for $z = a + ib \in \mathbb{C}$	(4.89)
$\lvert z \rvert$	$= \sqrt{a^2 + b^2}$ for $z = a + ib \in \mathbb{C}$	(4.89)
$\lvert a \rvert$	absolute value in an ordered ring	(1.87)

Symbol	Content	Introduced in
$\emptyset$	the empty set $\{ x \mid x \neq x \}$	-
#	number of elements of a set	
$\lvert X \rvert$	cardinality of the set X	section 0.3
	$= \#X$ for finite sets	
$X \cup Y$	$x \in$ union $\iff x \in X$ or $x \in Y$	section 0.3
$X \cap Y$	$x \in$ intersection $\iff x \in X$ and $x \in Y$	section 0.3
$\bigcup_{i \in I} X_i$	$x \in$ grand union $\iff \exists\, i \in I : x \in X_i$	section 0.3
$\bigcap_{i \in I} X_i$	$x \in$ grand intersection $\iff \forall\, i \in I : x \in X_i$	section 0.3
$X \times Y$	cartesian product of X and Y	(0.4)
$\prod_{i \in I} X_i$	cartesian product of all X_i (where $i \in I$)	section 0.3
$\mathcal{F}(X, Y)$	functions from X to Y	(0.5)
$\leq$	partial or total order	(0.17)
$\sim$	equivalence relation	(0.12)
$X/\sim$	X modulo $\sim$ = set of equivalence classes	(0.12)

Symbol	Content	Introduced in
A^*	set of maximal elements of the set A	(0.17)
A_*	set of minimal elements of the set A	(0.17)
R^*	group of invertible elements of the ring R	(1.45)
A^*	transpose matrix of the matrix A	(4.3)
$A^\#$	adjugate matrix of the matrix A	(4.61)
$\operatorname{cof}(A)$	cofactor matrix of the matrix A	(4.61)
$\overline{A}$	complex conjugate of the matrix A	(4.91)
	= the transpose matrix with conjugate entries	
φ'	adjoint homomorphism of φ	(4.99)

Part II

The Proofs

Chapter 14

List of Proofs

page	proof of	requirements
21	(0.4)	elementary

Chapter 15

All the Proofs

In this chapter we will finally present the proofs of all the statements (propositions, lemmas, theorems and corollaries) that have been given in the previous part. Note that the order of proofs is different from the order in which we gave the statements, though we have tried to stick to the order of the statements as tightly as possible. At some occasions a proof uses methods more advanced, than the current exposition of the topic. In this case the proof has to be postponed until general theory provides the arguments, that have been unavailable. In order to prevent circular conclusions we have to abstain from using these statements, until they can finally be proved. Hence we have taken great care to announce, when a proof cannot be done right away. And of course we do not use this particular statement before that.

15.1 Proofs of Chapter 0

Proof of (0.4):
If $u = x$ and $v = y$ it is clear that $\{u,v\} = \{x,y\}$ and hence $\{\, u,\{u,v\}\,\} = \{\, x,\{x,y\}\,\}$ as well. For the converse direction we need to distinguish two cases: **First case:** If $x = y$, then $\{x,y\} = \{x,x\} = \{x\}$ so in this case our assumption reads as:

$$\{\, u,\{u,v\}\,\} \;=\; \{\, x,\{x\}\,\}$$

That contains 2 assertions: $u \in \{\, x,\{x\}\,\}$ [which implies $u = x$ or $u = \{x\}$ and $\{u,v\} \in \{\, x,\{x\}\,\}$ [which implies $\{u,v\} = x$ or $\{\, u,v\,\} = \{x\}$]. Altogether we find 4 different combinations

	$u = x$	$u = \{x\}$
$\{u,v\} = x$	(1.A)	(1.B)
$\{u,v\} = \{x\}$	(1.C)	(1.D)

It will turn out, that 3 of these cases end in contradiction and the fourth case will yield what we need: In case (1.A) we have $u \in \{u,v\} = x = u$ which would mean $u \in u$ which contradicts the axiom of foundation. In case (1.B) we have $u \in \{u,v\} = x \in \{x\} = u$ such that $u \in x \in u$ which also contradicts the axiom of foundation. In case (1.C) we have $u = x$ and $\{x\} = \{u,v\} = \{x,v\}$. Thus $\{x,v\}$ contains one element only which means $x = v$. As we also have $x = y$ this is $y = x = v$ and hence $y = v$. In case (1.D) we have $u \in \{u,v\} = \{x\}$ such that $u = x$. But as also $x \in \{x\} = u = x$ we have $x \in x$ which contradicts the axiom of foundation, once more. Thus the first case leaves (1.C) only with $u = x$ and $v = y$.

If $u = v$ then we can interchange the roles of u, x and v, y respectively, so this has also been dealt with in the first case. So in the **second case** we may assume $u \neq v$ and $x \neq y$. In this case our assumption

$$\{\, u, \{u, v\}\,\} \;=\; \{\, x, \{x, y\}\,\}$$

contains the first assertion $u = x$ or $u = \{x, y\}$ and the second assertion: $\{u, v\} = x$ or $\{u, v\} = \{x, y\}$. Again we end up with 4 combinations to be considered

	$u = x$	$u = \{x, y\}$
$\{u, v\} = x$	(2.A)	(2.B)
$\{u, v\} = \{x, y\}$	(2.C)	(2.D)

Again it will turn out, that 3 of these cases end in contradictions and the fourth case will yield what we need: In case (2.A) we have $u \in \{u, v\} = x = u$ such that $u \in u$ contradicts the axiom of foundation. In case (2.B) we have $u \in \{u, v\} = x \in \{x, y\} = u$. Therefore $u \in x \in u$ is a contradiction to the axiom of foundation. In (2.C) we get $v \in \{u, v\} = \{x, y\}$. Therefore $v = x$ or $v = y$. But $v = x = u$ if untrue, as we are in case 2. Thus we have $v = y$ and $u = x$ as needed. In case (2.D) we have $u \in \{u, v\} = \{x, y\} = u$ such that $u \in u$ is our last contradiction to the axiom of foundation. Thus the second case leaves (2.C) only with $u = x$ and $v = y$, as well. □

Proof of (0.2):

- By definition for element of $x \in \bigcup_i (A_i \cap B)$ there is some $i \in I$ such that $x \in A_i \cap B$. In particular we get $x \in B$ and $x \in A_i$ for this $i \in I$. The latter is $x \in \bigcup_i A_i$ and as also $x \in B$ this means that x is contained in the set on the left-hand side. Conversely start with

 $$x \;\in\; \left(\bigcup_{i \in I} A_i \right) \cap B$$

 That is $x \in B$ and there is some $i \in I$ such that $x \in A_i$. For this i we get $x \in A_i \cap B$ and hence x is contained in the set on the right-hand side.

- By definition an element of $x \in \bigcap_i (A_i \cup B)$ satisfies $x \in A_i \cup B$ for any $i \in I$. Let us distinguish two cases: If $x \in B$ then x is already contained in the set on the left-hand side. And if $x \notin B$, then $x \in A_i \cup B$ implies $x \in A_i$. As this is true for any $i \in I$ we conclude $x \in \bigcap_i A_i$ such that x is contained in the set on the left-hand side again. Conversely start with

 $$x \;\in\; \left(\bigcap_{i \in I} A_i \right) \cup B$$

 If $x \in B$ then for any $i \in I$ we get $x \in A_i \cup B$ and hence x is contained in the set on the right-hand side. If $x \notin B$ then we necessarily have $x \in \bigcap_i A_i$ which means $x \in A_i$ for any $i \in I$. From this we trivially get $x \in A_i \cup B$, such that x is contained in the set on the right-hand side, in this case, as well.

- This identity is simpler than it looks, we just have to decode what it means for an x to be an element of the respective sets. So let's just do that

$$\begin{aligned} x \in \bigcup_{(i,j)\in I\times J} (A_i \cap B_j) &\iff \exists\,(i,j) \in I \times J \,:\, x \in A_i \cap B_j \\ &\iff \exists\, i \in I\ \exists\, j \in J \,:\, x \in A_i \text{ and } x \in B_j \\ &\iff \big(\exists\, i \in I \,:\, x \in A_i\big) \text{ and } \big(\exists\, j \in J \,:\, x \in B_j\big) \\ &\iff x \in \left(\bigcup_{i\in I} A_i\right) \cap \left(\bigcup_{j\in J} B_j\right) \end{aligned}$$

- For an x to be contained in $\bigcap_{(i,j)} (A_i \cup B_j)$ means $x \in A_i$ or $x \in B_j$ for any $(i,j) \in I \times J$. Likewise we can decode

$$x \;\in\; \left(\bigcap_{i\in I} A_i\right) \cup \left(\bigcap_{j\in J} B_j\right)$$

 to be the property $\forall\, i \in I : x \in A_i$ or $\forall\, j \in J : x \in B_j$. Thus if we start with such an x we may distinguish two cases: If $\forall\, i \in I : x \in A_i$ then $x \in A_i \cup B_j$ is satisfied trivially, for any $(i,j) \in I \times J$. Thus in this case x is contained in the right-hand set. And the same argument works out in the second case $\forall\, j \in J : x \in B_j$. Thus we have found the inclusion "$\subseteq$" and it remains to prove "$\supseteq$": Suppose x was *not* contained in the left-hand side set. Then there had to be some $i \in I$ and $j \in J$ such that $x \notin A_i$ and $x \notin B_j$. So for this combination $(i,j) \in I \times J$ we had $x \notin A_i \cup B_j$. But this contradicts the assumption that x is contained in $\bigcap_{(i,j)} (A_i \cup B_j)$.

- As $A_i \subseteq X$ we know that $x \notin A_i$ is equivalent to $x \in X \setminus A_i$. Using this both identities of the complements are straightforward to see, by elementary quantifier logic

$$\begin{aligned} x \in X \setminus \bigcup_{i\in I} A_i &\iff x \notin \bigcup_{i\in I} A_i \\ &\iff \textit{not}\ \ \forall\, i \in I \,:\, x \in A_i \\ &\iff \exists\, i \in I \,:\, x \notin A_i \\ &\iff x \in \bigcup_{i\in I} X \setminus A_i \\ x \in X \setminus \bigcap_{i\in I} A_i &\iff x \notin \bigcap_{i\in I} A_i \\ &\iff \textit{not}\ \ \exists\, i \in I \,:\, x \in A_i \\ &\iff \forall\, i \in I \,:\, x \notin A_i \\ &\iff x \in \bigcap_{i\in I} X \setminus A_i \end{aligned}$$

□

Proof of (0.7):

- By definition $f(A) = \{\, f(a) \mid a \in A \,\}$ that is $y \in f(A)$ is equivalent to $y = f(a)$ for some $a \in A$. Therefore we can rewrite the following set

$$\begin{aligned} f^{-1}\big(f(A)\big) &= \{\, x \in X \mid f(x) \in f(A) \,\} \\ &= \{\, x \in X \mid \exists\, a \in A : f(x) = f(a) \,\} \end{aligned}$$

And thereby A is contained in this set as for $x = a \in A$ we have $f(x) = f(a)$. If f is injective however, then $f(x) = f(a)$ for some $a \in A$ implies $x = a \in A$ such that this set is contained in A, as well. This is the first property, for the next two we just take a close look

$$\begin{aligned} f\big(f^{-1}(B)\big) &= \Big\{\, f(x) \mid x \in f^{-1}(B) \,\Big\} \\ &= \{\, f(x) \mid x \in X, f(x) \in B \,\} \\ &= \{\, b \in B \mid \exists\, x \in X : b = f(x) \,\} \\ &= B \cap \{\, y \in Y \mid \exists\, x \in X : y = f(x) \,\} \\ &= B \cap \{\, f(x) \mid x \in X \,\} \\ &= B \cap f(X) \\ f^{-1}\big(Y \setminus B\big) &= \{\, x \in X \mid f(x) \in Y \setminus B \,\} \\ &= \{\, x \in X \mid f(x) \notin B \,\} \\ &= X \setminus \{\, x \in X \mid f(x) \in B \,\} \\ &= X \setminus f^{-1}(B) \end{aligned}$$

- Next let us prove the equivalence of $f(A) \subseteq B$ and $A \subseteq f^{-1}(B)$: If we start with $f(A) \subseteq B$, then we have to consider any $a \in A$. Thus we have $f(a) \in f(A) \subseteq B$ by assumption, such that $f(a) \in B$. But $f^{-1}(B) = \{\, x \in X \mid f(x) \in B \,\}$ by definition, so $f(a) \in B$ means $a \in f^{-1}(B)$ and as this is true for any $a \in A$ we have $A \subseteq f^{-1}(B)$. Conversely, if we start with $A \subseteq f^{-1}(B)$ we have to consider any $y \in f(A) = \{\, f(a) \mid a \in A \,\}$. That is $y = f(a)$ for some $a \in A$ but by assumption $A \subseteq f^{-1}(B)$ this means $a \in f^{-1}(B)$ and thereby $f(a) \in B$. Thus $y \in f(A)$ implies $y = f(a) \in B$ and as this is true for any y, we have $f(A) \subseteq B$, as required.
- The properties for the preimage are always easy to verify: Recall the notation of the grand union $\bigcup \mathcal{B}$ to be the union $\bigcup_j B_j$ and compute

$$\begin{aligned} f^{-1}\left(\bigcup \mathcal{B}\right) &= \Big\{\, x \in X \mid f(x) \in \bigcup \mathcal{B} \,\Big\} \\ &= \{\, x \in X \mid \exists\, j \in J : f(x) \in B_j \,\} \\ &= \bigcup_{j \in J} \{\, x \in X \mid f(x) \in B_j \,\} \\ &= \bigcup_{j \in J} f^{-1}(B_j) \\ f^{-1}\left(\bigcap_{j \in J} B_j\right) &= \Big\{\, x \in X \mid f(x) \in \bigcap \mathcal{B} \,\Big\} \\ &= \{\, x \in X \mid \forall\, j \in J : f(x) \in B_j \,\} \\ &= \bigcap_{j \in J} \{\, x \in X \mid f(x) \in B_j \,\} \end{aligned}$$

$$= \bigcap_{j\in J} f^{-1}(B_j)$$

In the second part we already used the grand intersection $\bigcap \mathcal{B}$ which in complete analogy is $\bigcap_j B_j$. The respective properties for the image are a little harder to prove: Note that

$$\bigcup_{i\in I} f(A_i) \;=\; \bigcup_{i\in I} \{\, f(a_i) \mid a_i \in A_i \,\}$$

That is y is an element of this set if and only if there is some $i \in I$ and some $a_i \in A_i$ such that $y = f(a_i)$. On the other hand

$$f\left(\bigcup_{i\in I} A_i\right) \;=\; \{\, f(a) \mid \exists\, i \in I : a \in A_i \,\}$$

That is y is an element of this set if and only if there is some $i \in I$ and some $a \in A_i$ such that $y = f(a)$. Does sound familiar? Yep, it is just the same and hence the sets are equal. In the same manner we proceed with

$$\bigcap_{i\in I} f(A_i) \;=\; \{\, y \in Y \mid \forall\, i \in I\ \exists\, a_i \in A_i : y = f(a_i) \,\}$$

as $y \in f(A_i)$ if and only if there is some $a_i \in A_i$ with $y = f(a_i)$. The other set looks similar, but is not quite the same

$$f\left(\bigcap_{i\in I} A_i\right) \;=\; \{\, y \in Y \mid \exists\, a \in X : \forall\, i \in I : a \in A_i,\, y = f(a) \,\}$$

So if y is in this set, then there is some a with $a \in A_i$ for any $i \in I$ that also satisfies $y = f(a)$. In particular we can take $a_i := a$ and thereby see, that y is hence also contained in $\bigcap_i f(A_i)$, the converse inclusion need not be true however, as the a_i need not be the same a. However if f is injective, then we may fix some $j \in I$. Then for any other $i \in I$ we have $f(a_i) = y = f(a_j)$ such that $a_j = a_i \in A_i$. As this is true for any i we have $a := a_j \in \bigcap_i A_i$ which is the converse inclusion.

□

Proof of (0.10):
Injectivity: If (a) then for any $u, x \in X$ with $f(u) = f(x)$ we have $g(f(u)) = g(f(x))$. But by assumption $gf = \mathbb{1}_X$ we get $u = gf(u) = gf(x) = x$ which is (b) already. Next the implication (b) $\implies$ (c) has already been dealt with in (0.7). So for (c) $\implies$ (d) we start with some $y \in Y$. If there no $x \in X$ with $f(x) = y$ then $f^{-1}(\{\, y \,\}) = \emptyset$ so we have nothing to prove. If there is some $x \in X$ with $f(x) = y$ then we let $A := \{\, x \,\} \subseteq X$. Therefore $f(A) = \{\, f(x) \,\} = \{\, y \,\}$ and by assumption (c) we have $\{\, x \,\} = A = f^{-1}(f(A)) = f^{-1}(\{\, y \,\})$. That is $f^{-1}(\{\, y \,\})$ contains 0 or 1 element which is (d). To return from (d) to (a) we need to find some $g : Y \to X$ with $gf = \mathbb{1}_X$. To do this fix any $x_0 \in X$, then for any $y \in Y$ we define

$$g(y) \;:=\; \begin{cases} x_0 \text{ if } \#f^{-1}(\{\, y \,\}) = 0 \\ x \text{ if } \#f^{-1}(\{\, y \,\}) = 1 \end{cases} \quad \text{where} \quad \{\, x \,\} \;=\; f^{-1}(\{\, y \,\})$$

As we have (c) no other values of $\#f^{-1}(\{\,y\,\})$ may occur and hence g is a well-defined function. If now $y = f(x)$ then $x \in f^{-1}(\{\,y\,\})$ such that we get $g(y) = x$ Concatenating we get $x = g(y) = g(f(x)) = gf(x)$. And as this is true for any $x \in X$ we have found $gf = \mathbb{1}_X$ of (a).

Surjectivity: If (a) then for any $y \in Y$ we consider $x := g(y)$, then from $f(x) = fg(y) = y$ we see that $y \in f(X)$. As y has been arbitrary this is $Y \subseteq f(X) \subseteq Y$ and hence (b). In (0.7) we have seen that for any $B \subseteq Y$ and any $f : X \to Y$ we have $f(f^{-1}(B)) = B \cap f(X)$. Thus if (b) then we get $f(f^{-1}(B)) = B \cap f(X) = B \cap Y = B$ which is (c). Next for the implication (c) $\implies$ (d) we consider any $y \in Y$ and let $B := \{\,y\,\}$. Suppose there was some $y \in Y$ such that $\#f^{-1}(\{\,y\,\}) = 0$. This would mean $f^{-1}(B) = f^{-1}(\{\,y\,\}) = \emptyset$ and thereby $B = f(f^{-1}(B)) = f(\emptyset) = \emptyset$ which is a contradiction. Hence (c) implies (d). To return from (d) to (a) we need to find some $g : Y \to X$ with $fg = \mathbb{1}_Y$. To do this define

$$G \;:\; Y \;\to\; \mathcal{P}(X) \;:\; y \;\mapsto\; f^{-1}(\{\,y\,\})$$

By assumption $G(y) \subseteq X$ is non-empty for any $y \in Y$. Thus by the axiom of choice there is a function $g : Y \to X$ such that for any $y \in Y$ we have $g(y) \in G(y) = f^{-1}(\{\,y\,\})$. That is $f(g(y)) \in \{\,y\,\}$ and thereby $fg(y) = y$. As this is true for any $y \in Y$ we have $fg = \mathbb{1}_Y$ of (a).

Bijectivity: If (a) then we can define $f^{-1} : Y \to X$ by letting $f^{-1}(y) := x$ where $x \in X$ is the one and only x that satisfies $f(x) = y$. Then it is clear, that $f^{-1}(f(x)) = x$ as $f(x)$ satisfies $f(x) = f(x)$. That is $f^{-1}f = \mathbb{1}_X$. Also $f(f^{-1}(y)) = f(x)$ where $x \in X$ satisfies $f(x) = y$. That is $f(f^{-1}(y)) = y$ and therefore $ff^{-1} = \mathbb{1}_Y$. We sill have to prove the uniqueness of f^{-1} that is we consider any two functions $g, h : Y \to X$ such that $gf = \mathbb{1}_x = hf$ and $fg = \mathbb{1}_Y = fh$. Then for any $y \in Y$ we get

$$g(y) \;=\; g(fh(y)) \;=\; g(f(h(y)) \;=\; gf(h(y)) \;=\; h(y)$$

And as $g(y) = h(y)$ for any $y \in Y$ this is $g = h$. Now the implication (b) $\implies$ (c) is trivial, just let $\ell := f^{-1}$ and $r := f^{-1}$ then we are done. Also (c) $\implies$ (d) is clear, as both are the property (a) of an injective, resp. surjective function. To return from (d) to (a) we start with some $y \in Y$. As f is surjective property (b) tells us $Y = f(X) = \{\,f(x) \mid x \in X\,\}$. As $y \in Y$ this means there is some $x \in X$ with $y = f(x)$. For the uniqueness we use property (b) of injective functions: Suppose we had some x_1 and $x_2 \in X$ with $f(x_1) = y$ and $f(x_2) = y$. Then in particular $f(x_1) = f(x_2)$ such that $x_1 = x_2$. That is we found (d) from (a). □

Proof of (0.13):
We first need to verify that $X/\sim$ truly is a partition of X: First of all if $[x] \in X/\sim$ then $[x] \neq \emptyset$ as $x \sim x$ implies $x \in [x]$. Next we need to verify $[x] = [y]$ for any $[x], [y] \in X/\sim$ with $[x] \cap [y] \neq \emptyset$. To do this it suffices to check $[x] \subseteq [y]$, as by the same reasoning we get $[y] \subseteq [x]$. As $[x] \cap [y] \neq \emptyset$ there is some $u \in X$ with $u \in [x] \cap [y]$. By definition of $[x]$ this means $u \sim x$ and likewise $u \sim y$. But by the symmetry of $\sim$ this also is $x \sim u$. If now $z \in [x]$ is any element, then $z \sim x$, too. And thereby we get the chain $z \sim x$ and $x \sim u$ (which implies $z \sim u$) and $u \sim y$ such that $z \sim y$. This again is $z \in [y]$ and as z has been arbitrary this is $[x] \subseteq [y]$. Altogether we have proved property (2) of partitions. But property (3) is easy again: as $x \in [x]$ for any $x \in X$ we see that X is contained in the grand union of $X/\sim$.

Let us also prove that for any partition $\mathcal{A}$ of X the relation $\sim_{\mathcal{A}}$ truly is an equivalence relation: First of all, if $x \in X$ then there is some $A \in \mathcal{A}$ such that $x \in A$ by property (3) of partitions. Thereby $\{x,x\} = \{x\} \subseteq A$ such that $x \sim_{\mathcal{A}} x$. The symmetry of $\sim_{\mathcal{A}}$ is easy: Suppose $x \sim_{\mathcal{A}} y$ that is $\{x,y\} \subseteq A$ for some $A \in \mathcal{A}$. As $\{y,x\} = \{x,y\}$ we also have $\{y,x\} \subseteq A$ such that $y \sim_{\mathcal{A}} x$, as well. Finally we have to verify the transitivity: That is we consider $x \sim_{\mathcal{A}} y$ and $y \sim_{\mathcal{A}} z$. By construction there are some $A, B \in \mathcal{A}$ such that $\{x,y\} \subseteq A$ and $\{y,z\} \subseteq B$. In particular $y \in A \cap B$ such that $A \cap B \neq \emptyset$ implies $A = B$. But then we have $\{x,z\} \subseteq \{x,y,z\} \subseteq A = B$ such that $x \sim_{\mathcal{A}} z$, as well.

So far we have seen that both $\sim \mapsto X/\sim$ and $\mathcal{A} \mapsto \sim_{\mathcal{A}}$ are well defined maps. To prove that $\sim \mapsto X/\sim$ is bijective it suffices to show that $\mathcal{A} \mapsto \sim_{\mathcal{A}}$ is the inverse map. For the one direction we need to show: If we start with $\sim$ and let $\mathcal{A} := X/\sim$ then we have $\sim = \sim_{\mathcal{A}}$. That is we have to prove the following equivalence for any $x, y \in X$

$$x \sim y \iff x \sim_{\mathcal{A}} y$$

For the implication from left to right we have $x \sim y$ which is $x \in [y]$. As $y \in [y]$ is generally true we find $\{x,y\} \subseteq [y]$ such that $x \sim_{\mathcal{A}} y$. If conversely $x \sim_{\mathcal{A}} y$ then $\{x,y\} \subseteq [z]$ for some $z \in X$. In particular $x \sim z$ and $y \sim z$. But as $\sim$ is an equivalence relation this also is $z \sim y$ and hence $x \sim y$. Thus we have the equivalence of the statements. And thus we found $\sim \mapsto \mathcal{A} := X/\sim \mapsto \sim_{\mathcal{A}} = \sim$ For the other direction we need to show: If we start with $\mathcal{A}$ then

$$\mathcal{A} = {}^{X}\big/_{\sim_{\mathcal{A}}}$$

As the equivalence relation now is $\sim_{\mathcal{A}}$ let us write $[x]_{\mathcal{A}}$ for the equivalence class of $x \in X$, that is $[x]_{\mathcal{A}} = \{u \in X \mid u \sim_{\mathcal{A}} x\}$. If $A \in \mathcal{A}$ then there is some $x \in A$, as $A \neq \emptyset$. We will now prove that

$$x \in A \implies A = [x]_{\mathcal{A}}$$

For the inclusion $A \subseteq [x]_{\mathcal{A}}$ we consider any $a \in A$, as $x \in A$ as well this means $\{a,x\} \subseteq A$ such that $a \sim_{\mathcal{A}} x$ which again is $a \in [x]_{\mathcal{A}}$. Conversely if $u \in [x]_{\mathcal{A}}$ then we have $u \sim_{\mathcal{A}} x$ which in turn is $\{u,x\} \subseteq B$ for some $B \in \mathcal{A}$. But as $x \in A$ and $x \in B$ we have $x \in A \cap B$ and therefore $B = A$ by property (2) of the partition $\mathcal{A}$. In particular we see $u \in B = A$ such that $[x]_{\mathcal{A}} \subseteq A$, as well.
So if $A \in \mathcal{A}$ then $A = [x]_{\mathcal{A}}$ for some $x \in X$ and thereby $A \in X/\sim_{\mathcal{A}}$. If conversely $[x]_{\mathcal{A}}$ is any equivalence class of $\sim_{\mathcal{A}}$ then $x \sim_{\mathcal{A}} x$ implies $x \in \{x,x\} \subseteq A$ for some $A \in \mathcal{A}$. Now $x \in A$ implies $A = [x]_{\mathcal{A}}$ again, such that $[x]_{\mathcal{A}} = A \in \mathcal{A}$. That is these two partitions are equal and altogether we have verified that $\mathcal{A} \mapsto \sim_{\mathcal{A}} \mapsto X/\sim_{\mathcal{A}} = \mathcal{A}$. That is the maps $\sim \mapsto X/\sim$ and $\mathcal{A} \mapsto \sim_{\mathcal{A}}$ are mutually inverse. In particular they are bijective which we had to prove. □

Proof of (0.19):
Let $F = \{x_1, \ldots, x_n\}$, then we will prove the claims by induction on n: For $n = 1$ we have $F^* = \{x_1\}$ and $\max(F) = x_1$ as there is no other element of F to compare it with. For the induction step let $F_0 := \{x_1, \ldots, x_{n-1}\}$ such that $F = F_0 \cup \{x_n\}$.

First consider a total order $\leq$: If $x_i \leq x_n$ for any $1 \leq i < n$ then $\max(F) = x_n$. Otherwise (as $\leq$ is total) there is some x_i with $x_n \leq x_i$. And by induction hypothesis F_0 has a greatest element g. Therefore $x_n \leq x_i \leq g$ implies $x_n \leq g$. Thus $\max(F) = g$. In both cases F has a greatest element, as claimed.

Now consider a partial order $\leq$: By induction hypothesis F_0 has a maximal element m. If now $m \leq x_n$ then x_n is a maximal element: Suppose $x_n \leq f$ for some $f \in F_0$. Then $m \leq x_n \leq f$ implies $m \leq f$ and hence $m = f$, as m was maximal in F_0. Then $f = m \leq x_n \leq f$ implies $x_n = f$. Conversely if $\neg(x \leq x_n)$ then m is a maximal element: If $f \in F$ is any set then either $f \in F_0$ for which we have $m \leq f \implies f = m$ due to the maximality of m in F_0 or $f = x_n$. But in the latter case $m \leq f$ is untrue, so there is nothing to prove. In both cases F has a maximal element, which had to be shown.

The respective statements for the least element and minimal elements of F follow immediately if we consider the opposite order $x \leq' y \iff y \leq x$. □

Proof of (0.20):
First of all it suffices to to prove this for minima, as the same property for maxima follows by going to the inverse relation $x \geq y \iff y \leq x$. Let us first distinguish the case $n = 2$: As $\min\{ x_1 \} = x_1$ we get $\min\{ \min\{ x_1 \}, x_2 \} = \min\{ x_1, x_2 \}$ and likewise $\min\{ x_1, \min\{ x_2 \} \} = \min\{ x_1, x_2 \}$.
Now for $n \geq 3$ we will distinguish two cases: First of all assume $\min\{ x_1, \ldots, x_n \} = x_n$ and let $x_m = \min\{ x_1, \ldots, x_{n-1} \}$. Then by assumption $x_n \leq x_i$ for any $i \in 1 \ldots (n-1)$ and in particular $x_n \leq x_m$ such that

$$\min\{ \min\{ x_1, \ldots, x_{n-1} \}, x_n \} = \min\{ x_m, x_n \} = x_n = \min\{ x_1, \ldots, x_n \}$$

Also, as $x_n \leq x_i$ for any $i \in 2 \ldots n$ we have $\min\{ x_2, \ldots, x_n \} = x_n$ and as also $x_n \leq x_1$ we have $\min\{ x_1, x_n \} = x_n$ as well. From this we also get the equality

$$\min\{ x_1, \min\{ x_2, \ldots, x_n \} \} = \min\{ x_1, x_n \} = x_n = \min\{ x_1, \ldots, x_n \}$$

Conversely let $x_m = \min\{ x_1, \ldots, x_n \}$ be the minimal element and assume $x_m < x_{n+1}$. Then in particular $x_m = \min\{ x_1, \ldots, x_{n-1} \}$ and $\min\{ x_m, x_n \} = x_m$ such that we find

$$\min\{ \min\{ x_1, \ldots, x_{n-1} \}, x_n \} = \min\{ x_m, x_n \} = x_m = \min\{ x_1, \ldots, x_n \}$$

For the second equality we first note $x_m = \min\{ x_2, \ldots, x_m \}$ again and as also $x_m \leq x_1$ such that $\min\{ x_1, x_m \} = x_m$ from which we conclude once more

$$\min\{ x_1, \min\{ x_2, \ldots, x_n \} \} = \min\{ x_1, x_m \} = x_m = \min\{ x_1, \ldots, x_n \}$$

□

Proof of (0.21):
Consider any to $x, y \in \bigcap_i C_i$ - as I is non-empty there is some $i \in I$ and hence $x, y \in C_i$. But as $C_i \subseteq X$ is a chain this implies $x \leq y$ or $y \leq x$. And as this is true for any $x, y \in \bigcap_i C_i$ we find, that $\bigcap_i C_i \subseteq X$ is a chain in X again.
Consider any to $x, y \in \bigcup_i C_i$ - that is $x \in C_i$ and $y \in C_j$ for some $i, j \in I$. As the C_i form a net under inclusion there is some $k \in I$ such that $C_i \subseteq C_k$ and $C_j \subseteq C_k$. In particular $x \in C_i \subseteq C_k$ implies $x \in C_k$ and likewise $y \in C_k$. But as $C_k \subseteq X$ is a chain this implies $x \leq y$ or $y \leq x$. And as this is true for any $x, y \in \bigcup_i C_i$ we find, that $\bigcup_i C_i \subseteq X$ is a chain in X again. □

Proof of (0.22):
Let us first verify the equivalence of (a) and (b): For (a) $\implies$ (b) consider any $x \in X$ and let $y := f(x)$. Then $y \leq f(x)$ is a given such that (a) implies $x \leq g(y) = gf(x)$. Likewise for any $y \in Y$ we let $x := g(y)$ such that (a) also yields $y \leq f(x) = fg(y)$ from $x \leq g(y)$.Conversely for (b) $\implies$ (a) we start with $x \leq g(y)$. As f is anti-tonous, this implies $f(x) \geq fg(y) \geq y$ by (b) and hence $y \leq f(x)$. Likewise $y \leq f(x)$ implies $g(y) \geq gf(x) \geq x$ such that $x \leq g(y)$.

Next we prove that (a) and (b) $\implies$ (c): For any $x \in X$ let $Y_x := \{\, y \in Y \mid x \leq g(y) \,\}$, then we have to verify $f(x) = \max(Y_x)$. First of all we have $x \leq gf(x) = g(f(x))$ by (b), which means $f(x) \in Y_x$. And if we pick up any $y \in Y_x$ then $x \leq g(y)$ implies $y \leq f(x)$ due to (a). Thus $f(x)$ is a greatest element of Y_x.

Reversing the roles of f and g we likewise find that $g(y)$ is a maximal element of $X_y := \{\, x \in X \mid y \leq f(x) \,\}$. The same reasoning shows (c) $\implies$ (a): Since $f(x)$ is a greatest element of Y_x we find that $x \leq g(y)$ is $y \in Y_x$ and hence $y \leq f(x)$. Again reversing the roles turns $y \leq f(x)$ into $x \in X_y$ and hence $x \leq g(y)$. Thus we have established the equivalence of (a) and (c), as well.

Let us now prove, that (b) implies $fgf = f$ and $gfg = g$: We start with $x \leq gf(x)$, as f is anti-tonic we get $f(x) \geq f(gf(x)) = fg(f(x)) \geq f(x)$, where we used (b) again. Together $f(x) \geq fgf(x) \geq f(x)$ implies $fgf(x) = f(x)$. Likewise $y \leq fg(y)$ turns into $g(y) \geq g(fg(y)) = fg(g(y)) \geq g(y)$ such that $g(y) \geq fgf(y) \geq g(y)$ also is $fgf(y) = g(y)$.

And from this property we get the one-to-one correspondence of the images: We note that by $g(Y) \subseteq X$ we have $f(g(Y)) \subseteq f(X)$ and therefore the map $f : g(Y) \to f(X)$ is well-defined. Likewise $g : f(X) \to g(Y)$ is well-defined. Now consider any $x = f(y) \in g(Y)$, then $gf(x) = gfg(y) = g(y) = x$, that is gf is the identity map on $g(Y)$. In complete analogy we find for any $y = f(x) \in f(X)$ that $fg(y) = fgf(x) = f(x) = y$ such that fg is the identity map on $f(X)$. That means that f and g are mutually inverse $f = g^{-1}$ and hence form a one-to-one correspondence. □

Proof of (0.25):
Let us prove the equivalences for the ACC first: The implication (a) $\implies$ (b) is quite easy to see: Given an ascending chain $(x_k) \subseteq X$ (where $k \in \mathbb{N}$), that is $x_0 \leq x_1 \leq x_2 \leq \ldots$, let us take $A := \{\, x_k \mid k \in \mathbb{N} \,\}$. By assumption A has a maximal element $a^* \in A$. Pick up some $s \in \mathbb{N}$ such that $a^* = x_s$. If now $i \in \mathbb{N}$, then (as (x_k) is an ascending chain) we have $x_s \leq x_{s+i}$. But due to the maximality of $x_s = a^*$ this already is $x_{s+i} = x_s$.

The implication (b) $\implies$ (a) will be proved as $\neg$ (a) $\implies$ $\neg$ (b), which is only slightly more difficult: As (a) is untrue there is some non-empty subset $A \subseteq X$ without maximal element. Negating the statement that A contains a maximal element yields:

$$\forall\, a \in A\ \exists\, b \in A\ :\ a < b$$

That is (by the axiom of choice) we may pick up a map $\nu : A \to A$ such that $\nu(a) := b$ for some $b \in A$ with $a < b$. And as A is non-empty we may start with some $x_0 \in A$. Now recursively define $x_{k+1} := \nu(x_k) = \nu^k(x_0)$. Then by construction we have found an infinitely ascending chain of elements $x_0 < x_1 < x_2 < \ldots$ which is the negation of (a).

For the equivalences of of the DCC we take $(X, \geq)$ as a partially ordered set under the inverse order $x \geq y \ :\Longleftrightarrow \ y \leq x$. A minimal element of $\leq$ is a maximal element of $\geq$. And the DCC for $\leq$ is the ACC for $\geq$. We already have already established the equivalence of (a) and (b) for the ACC of $(X, \geq)$, so this is the equivalence of (a) and (b) for the DCC of $(X, \leq)$. □

Proof of (0.26):
Let us first prove (a) $\implies$ (c): So consider any chain $C \subseteq X$, if $C = \emptyset$, then it is finite, so we may assume $C \neq \emptyset$. We will construct an ascending sequence of elements, to do so start with $C_0 := C$. As $C_0 \neq \emptyset$ and $(X, \leq)$ satisfies DCC we may choose a minimal element in C_0

$$x_0 \ \in \ \big(C_0\big)_*$$

Suppose we already have $x_0, x_1, \ldots, x_n \in C$ such that $x_0 < x_1 < \cdots < x_n$ then we continue with $C_{n+1} := C \setminus \{ x_0, x_1, \ldots, x_n \}$. If still $C_{n+1} \neq \emptyset$ then we may choose a minimal element again

$$x_{n+1} \ \in \ \big(C_{n+1}\big)_*$$

Suppose we had $x_{n+1} \leq x_n$ then, as $x_{n+1} \in C_{n+1} \subseteq C_n$ and x_n is minimal in C_n this would imply $x_{n+1} = x_n$. But then $x_n \in C_{n+1}$ which is untrue by construction of C_{n+1}. But as $x_{n+1} \leq x_n$ is false, then $x_n < x_{n+1}$ as any two elements of C are comparable. Thus we are able to construct a strictly increasing chain of elements

$$x_0 \ < \ x_1 \ < \ \ldots \ < \ x_n \ < \ x_{n+1}$$

of arbitrary length. But as $(X, \leq)$ also satisfies ACC there is no infinite strictly increasing sequence in X. That means, that at some stage $s \in \mathbb{N}$ we cannot continue to append elements and this only is the case if $C_{s+1} = \emptyset$. But this means that $C = \{ x_0, x_1, \ldots, x_s \}$ is a finite set.

Next we will prove (c) $\implies$ (b): Starting with an ascending sequence of finite chains $C_0 \subseteq C_1 \subseteq C_2 \subseteq \ldots$ in X we need to show that this chain stabilizes eventually. Let us define

$$C \ := \ \bigcup_{k=0}^{\infty} C_k \ \subseteq \ X$$

As $(C_k) \subseteq \mathcal{C}_0(X, \leq)$ is totally ordered under $\subseteq$ and any $C_k \subseteq X$ is a chain (0.21) tells us, that $C \in \mathcal{C}(X, \leq)$ is a chain again. But by assumption (c) C then is finite. As any $C_k \subseteq C$ we find an increasing sequence in $\mathbb{N}$

$$\#C_0 \ \leq \ \#C_1 \ \leq \ \#C_2 \ \leq \ \ldots \ \leq \ \#C \ < \ \infty$$

As C contains finitely many elements, this sequence in $\mathbb{N}$ is bound and cannot rise indefinitely. Thus there is some $s \in \mathbb{N}$ such that $\#C_{s+i} = \#C_s$ for any $i \in \mathbb{N}$. And this is $C_{s+i} = C_s$ as we also have $C_s \subseteq C_{s+i}$ and these are finite sets.

To go full circle we need to prove (b) $\implies$ (a): We start by proving that $(X, \leq)$ satisfies ACC, as well. To do this consider an ascending sequence $x_0 \leq x_1 \leq x_2 \leq \ldots$ in X and denote $C_k := \{ x_0, x_1, \ldots, x_k \} \subseteq X$. Then clearly $C_k \in \mathcal{C}_0(X, \leq)$ and

$$C_0 \ \subseteq \ C_1 \ \subseteq \ C_2 \ \subseteq \ \ldots$$

is an ascending sequence in $\mathcal{C}_0(X,\leq)$. By assumption there is some $s \in \mathbb{N}$ such that for any $i \in \mathbb{N}$ we have $C_{s+i} = C_s$. That is $x_{s+i} \in C_{s+i} = C_s = \{ x_0, x_1, \ldots, x_s \}$ and thereby $x_{s+i} = x_k$ for some $k \in 0 \ldots s$. Then $x_{s+i} = x_k \leq x_s \leq x_{s+i}$ implies $x_{s+i} = x_s$. That is the sequence (x_k) stabilizes. For the DCC we consider $x_0 \geq x_1 \geq x_2 \geq \ldots$ in X again. With the same C_k as before we find $C_{s+i} = C_s$ again and thereby $x_{s+i} = x_k \geq x_s \geq x_{s+i}$. In complete analogy we get $x_{s+i} = x_s$ such that $(X,\leq)$ also satisfies the DCC.
It remains to prove that in this case any chain $C \in \mathcal{C}(X,\leq)$ can be refined to a maximal, finite chain in X. By (c) we know that $C = \{ x_1, \ldots, x_n \}$ is finite. Now let $\mathcal{A}$ be the set of all finite chains in X containing C

$$\mathcal{A} \;:=\; \{ D \in \mathcal{C}_0(X,\leq) \mid C \subseteq D \}$$

Then $\mathcal{A} \neq \emptyset$, as $C \in \mathcal{A}$. And by (b) $\mathcal{C}_0(X,\leq)$ satisfies the ACC, such that there is a maximal chain $C^* \in \mathcal{A}^*$. And if $D \in \mathcal{C}_0(X,\leq)$ satisfies $C^* \subseteq D$ then (as $C \subseteq C^*$) we have $D \in \mathcal{A}$, such that the maximality of C^* in $\mathcal{A}$ implies $C^* = D$. □

Proof of (0.27):
The proof is elementary, but makes use of the axiom of choice and is *very* intricate. For better readability we broke it down into several steps:

(0) If $X = \emptyset$ then $M = \emptyset$ is a chain (all elements of $\emptyset$ are comparable) that also is maximal (X does not have any other subsets). So the claim is satisfied trivially. From now on consider $X \neq \emptyset$:

(1) In a first step we will construct a function $\mathcal{C}(X,\leq) \to \mathcal{C}(X,\leq)$ that maps $C \mapsto C'$ where we have to construct C': To do this start with $\mathcal{A} := \mathcal{P}(X) \setminus \{ \emptyset \}$. Then $\mathcal{A} \neq \emptyset$, as $X \in \mathcal{A}$ and for the same reason we have $X \subseteq \bigcup \mathcal{A} \subseteq X$. Thus (by the axiom of choice) there is a choice function $r : \mathcal{A} \to X$ such that for any $A \in \mathcal{A}$ we have $r(A) \in A$. Given a chain $C \in \mathcal{C}(X,\leq)$, let us denote

$$C^+ \;:=\; \{ x \in X \setminus C \mid C \cup \{ x \} \in \mathcal{C}(X,\leq) \}$$

That is C^+ is the set of all elements, that can be appended to C without ruining its chain property. It may well be, that C^+ is empty - in fact we are looking for a a chain M with this property. If not, that is $C^+ \neq \emptyset$, then $C^+ \in \mathcal{A}$ and hence we may define

$$C' \;:=\; \begin{cases} C \text{ if } C^+ = \emptyset \\ C \cup \{ r(C^+) \} \text{ if } C^+ \neq \emptyset \end{cases}$$

In either case we have $C \subseteq C'$. And if $C \subset C'$ then the one elements that was appended, is $r(C^+) \in C^+$. This means that C' is a chain again and hence this function is well-defined.

(2) Fix any $x_0 \in X$ (this is possible, since $X \neq \emptyset$, according to step (0). Then $\{ x_0 \}$ is a chain of X, albeit a very short one.

$$\{ x_0 \} \;\in\; \mathcal{C}(X,\leq)$$

If $\mathcal{T} \subseteq \mathcal{C}(X,\leq) \subseteq \mathcal{P}(X)$ then $\mathcal{T}$ is partially ordered under inclusion $\subseteq$. Thus it makes sense to speak of chains (under $\subseteq$) of chains (under $\leq$) of X. I.e. we regard the set $\mathcal{C}(\mathcal{T},\subseteq) \subseteq \mathcal{P}(\mathcal{P}(X))$.

(3) **Definition:** As set of chains $\mathcal{T} \subseteq \mathcal{C}(X, \leq)$ will be said to be a **tower**, iff it satisfies all of the following three properties:

(T1) $\{ x_0 \} \in \mathcal{T}$

(T2) $\forall\, T \in \mathcal{T} \,:\, T' \in \mathcal{T}$

(T3) $\forall\, A \in \mathcal{C}(\mathcal{T}, \subseteq) \,:\, \mathcal{A} \neq \emptyset \implies \bigcup \mathcal{A} \in \mathcal{T}$

(4) For the fixed $x_0 \in X$ let us now define the following set of chains of X

$$\mathcal{T}_0 \;:= \{\, T \in \mathcal{C}(X, \leq) \mid x_0 \in T \,\}$$

We will now prove that $\mathcal{T}_0$ is a tower: As $\{ x_0 \}$ is a chain and $x_0 \in \{ x_0 \}$ we have (T1). If $T \in \mathcal{T}_0$ then $x_0 \in T \subseteq T'$ such that (T2) is satisfied, too. Now consider some $A \subseteq \mathcal{C}(\mathcal{T}_0, \subseteq)$ with $A \neq \emptyset$, then we need to prove $T := \bigcup A \in \mathcal{T}_0$. First we prove that $T \in \mathcal{C}(X, \leq)$ is a chain of X: That is any two elements $a, b \in T$ have to be comparable. By construction $a \in T$ means $a \in A$ for some $A \in \mathcal{A}$ and likewise $b \in B$ for some $B \in \mathcal{A}$. As $\mathcal{A}$ is a chain its elements A and B are comparable. Without loss of generality say $A \subseteq B$. Then $a \in A \subseteq B$ implies $a \in B$. But we also have $b \in B$ and as $B \in \mathcal{A} \subseteq \mathcal{T}_0 \subseteq \mathcal{C}(X, \leq)$ we see that $B \subseteq X$ is a chain in X. That is a and b are comparable. And as a and b have been arbitrary elements of T this means $T \in \mathcal{C}(X, \leq)$ is a chain itself. But as $A \in \mathcal{A} \subseteq \mathcal{T}_0$ we have $x_0 \in A$ by construction of $\mathcal{T}_0$. Hence we find $x_0 \in A \subseteq T$ such that $T \in \mathcal{T}_0$ which had to be shown for (T3).

(5) By (4) we know that towers are not a void notion, there is at least on of these. So we are tempted to look at the smalles tower possible

$$\mathcal{T}_* \;:= \bigcap \{\, \mathcal{T} \subseteq \mathcal{C}(X, \leq) \mid \mathcal{T} \text{ is a tower} \,\}$$

We will prove that $\mathcal{T}_*$ is a tower again: As for any tower $\mathcal{T}$ we have $\{ x_0 \} \in \mathcal{T}$ by (T1), we also have $\{ x_0 \} \in \mathcal{T}_*$. This is (T1) for $\mathcal{T}_*$. And if $T \in \mathcal{T}_*$ then $T \in \mathcal{T}$ for any tower $\mathcal{T}$. Thereby $T' \in \mathcal{T}$ again, for any tower $\mathcal{T}$ such that $T' \in \mathcal{T}_*$ as well. This is (T2) for $\mathcal{T}_*$. Finally take some $\mathcal{A} \in \mathcal{C}(\mathcal{T}_*, \subseteq)$ with $\mathcal{A} \neq \emptyset$ again and let $T := \bigcup \mathcal{A} \subseteq X$. That is $\mathcal{A} \subseteq \mathcal{T}_*$ is a chain. And for any tower $\mathcal{T}$ we have $\mathcal{A} \subseteq \mathcal{T}_* \subseteq \mathcal{T}$ such that $T \in \mathcal{T}$. As this is true for any tower we have $T \in \mathcal{T}_*$ which finally is (T3) for $\mathcal{T}_*$.

(6) Let $C \in \mathcal{T}_*$ be a chain that is comparable to any other chain, that is $C \subseteq T$ or $T \subseteq C$ for any other $T \in \mathcal{T}_*$. Then we define:

$$\mathcal{T}_C \;:= \; \left\{\, T \in \mathcal{T}_* \mid C' \subseteq T \text{ or } T \subseteq C \,\right\}$$

We will prove that $\mathcal{T}_C$ is another tower: As $\mathcal{T}_*$ is a tower we have $\{ x_0 \} \in \mathcal{T}_*$. And as $C \in \mathcal{T}_* \subseteq \mathcal{T}_0$ we have $x_0 \in C$ due to the construction of $\mathcal{T}_0$. Thus $\{ x_0 \} \subseteq C$ such that $\{ x_0 \} \in \mathcal{T}_C$. This is (T1) for $\mathcal{T}_C$. If now $T \in \mathcal{T}_C$ then we have to show $T' \in \mathcal{T}_C$ that is $C' \subseteq T'$ or $T' \subseteq T$. By assumption $T \in \mathcal{T}_C$ we have $C' \subseteq T$ or $T \subseteq C$. In the first case $C' \subseteq T \subseteq T$ we are done already. In the second case $T \subseteq C$ we need to recall our assumption on C: As $\mathcal{T}_*$ is a tower, we have $T' \in \mathcal{T}_*$ and thereby C is comparable with T'. We either have $C \subseteq T'$ or $T' \subseteq C$. The second case $T' \subseteq C$ is one of the good options, it yields $T' \in \mathcal{T}_C$ directly. Thus we are stuck with

$T \subseteq C$ and $C \subseteq T'$. As T' exceeds T by exactly one point $[T' = T \cup \{ x \}$ for $x = r(T^+) \in X]$ we either have $C = T$ or $C = T'$. The first is $C' = T'$ in particular $C' \subseteq T'$ and the second is $T' \subseteq C$ in particular. Thus in both cases we find $C' \subseteq \mathcal{T}_C$ again. Thus we have proved (T2) for $\mathcal{T}_C$. Let now $\mathcal{A} \subseteq \mathcal{T}_C$ with $\mathcal{A} \neq \emptyset$. In particular $\mathcal{A} \subseteq \mathcal{T}_*$ such that $T := \bigcup \mathcal{A} \in \mathcal{T}_*$, since $\mathcal{T}_*$ is a tower. By assumption on C it is comparable with any element $A \in \mathcal{A}$. If we have $A \subseteq C$ for any $A \in \mathcal{A}$ then $T = \bigcup A \subseteq C$ such that $T \in \mathcal{T}_C$. So let us now consider the case that there is some $B \in \mathcal{A}$ with $C \subseteq B$. As $B \in \mathcal{A} \subseteq \mathcal{T}_C$ we have $C' \subseteq B$ - the other option $B \subseteq C$ has been ruled out. In particular $C' \subseteq B \subseteq \bigcup \mathcal{A} = T$ such that we also have $T \in \mathcal{T}_C$ in this case. That is (T3) for $\mathcal{T}_C$

(7) Let us now introduce the following subset of $\mathcal{T}_*$ - it consist of all the elements of $\mathcal{T}_*$ that are comparable with every other element of $\mathcal{T}_*$

$$\mathcal{C}_* \;:=\; \{ A \in \mathcal{T}_* \mid \forall B \in \mathcal{T}_* : A \subseteq B \text{ or } B \subseteq A \}$$

We will now prove, that $\mathcal{C}_*$ is a tower, too: As $\mathcal{T}_*$ is a tower we have $\{ x_0 \} \in \mathcal{T}_*$. And if $T \in \mathcal{T}_*$ is any other element of $\mathcal{T}_* \subseteq \mathcal{T}_0$ we find $x_0 \in T$ due to the construction of $\mathcal{T}_0$. Thus $\{ x_0 \} \subseteq T$ and hence $\{ x_0 \}$ is comparable with all other $T \in \mathcal{T}_*$. This is $\{ x_0 \} \in \mathcal{C}_*$ and hence (T1) for $\mathcal{C}_*$. If now $C \in \mathcal{C}_*$ then $\mathcal{C}_C$ is a tower according to (6). In particular we have $\mathcal{T}_* \subseteq \mathcal{T}_C$ by construction of $\mathcal{T}_*$. But as also $\mathcal{T}_C \subseteq \mathcal{T}_*$ by construction of $\mathcal{T}_C$ this is $\mathcal{T}_C = \mathcal{T}_*$. That is for any $B \in \mathcal{T}_*$ we have $C' \subseteq B$ or $B \subseteq C \subseteq C'$. That is C' is comparable with any $B \in \mathcal{T}_*$ and hence $C' \in \mathcal{C}_*$ again. This is (T2) for $\mathcal{C}_*$. Let now $\mathcal{A} \subseteq \mathcal{C}_*$ with $\mathcal{A} \neq \emptyset$. In particular $\mathcal{A} \subseteq \mathcal{T}_*$ such that $T := \bigcup \mathcal{A} \in \mathcal{T}_*$, since $\mathcal{T}_*$ is a tower. Now consider any $B \in \mathcal{T}_*$ if $A \subseteq B$ for any $A \in \mathcal{A}$ then $T = \bigcup \mathcal{A} \subseteq B$ and hence T and B are comparable. If there is some $A \subseteq \mathcal{B}$ with $\neg(A \subseteq B)$ then we note that $A \in \mathcal{A} \subseteq \mathcal{C}_*$, that is A is comparable with *any* element of $\mathcal{T}_*$. And since $\neg(A \subseteq B)$ this only leaves $B \subseteq A$ for this particular $A \in \mathcal{A}$. Thus $B \subseteq A \subseteq \bigcup \mathcal{A} = T$. Thus B and T also are comparable in this case such that T is comparable with any $B \in \mathcal{T}_*$. But this is precisely what it takes for $T \in \mathcal{C}_*$. Thus we have proved (T3) for $\mathcal{C}_*$.

(8) Let us now reap the harvest of (7): Since $\mathcal{C}_*$ is a tower we have $\mathcal{T}_* \subseteq \mathcal{C}_*$ by construction of $\mathcal{T}_*$. But as $\mathcal{C}_* \subseteq \mathcal{T}_*$ has been a subset of $\mathcal{T}_*$ this is $\mathcal{C}_* = \mathcal{T}_*$. By construction of $\mathcal{C}_*$ this means that *every* element of $\mathcal{T}_*$ is comparable, that is $\mathcal{T}_*$ is totally ordered under $\subseteq$, we have

$$A \;\subseteq\; B \quad \text{or} \quad B \;\subseteq\; A$$

for any $A, B \in \mathcal{T}_*$. Finally define $M := \bigcup \mathcal{T}_*$ as we have just seen $\mathcal{T}_*$ is a chain itself, property (T3) of the tower $\mathcal{T}_*$ implies $M \in \mathcal{T}_*$ again. So by property (T2) we also have $M' \in \mathcal{T}_*$ such that $M' \subseteq \bigcup \mathcal{T}_* = M \subseteq M'$. So at long last we have $M' = M$. By construction of M' this is the case if and only if $M^+ = \emptyset$. So consider any $C \in \mathcal{C}(X, \leq)$ such that $M \subseteq C$. If there was some $x \in C \setminus M$ then $M \cup \{ x \} \subseteq C$ would be totally ordered, as it is a subset of the totally ordered set C. So we would have $x \in M^+ = \emptyset$ which is absurd. Hence we have $C = M$, which finally is the maximality of M.

□

Proof of (0.28):
By Hausdorff's maximum principle (0.27) Z has a maximal chain $M \subseteq Z$. By assumption (2) M has an upper bound $m \in Z$. That is we have $z \leq m$ for any $z \in M$. We will prove that m is a maximal element of Z: Suppose there was some $z \in Z$ with $m \leq z$. Then $M' := M \cup \{ z \}$ is a chain again: Given any $x, y \in M'$ we have four possibilities: (P1) $x, y \in M$, then x and y are comparable, as M is a chain; (P2) $x \in M$ but $y = z$ then $x \leq m \leq z$ such that $x \leq z = y$ are comparable; (P3) $x = z$ but $y \in M$ is analogous to (P2) and (P4) $x = z$ and $y = z$. Then $x = y$ trivially are comparable. In any case x and y are comparable and therefore $M' \subseteq Z$ is another chain in Z with $M \subseteq M'$. By maximality of M we have $M' = M$ which is $z \in M$. As m is an upper bound of M this implies $z \leq m$ and hence $z = m$. □

Proof of (0.30):
If $X = \emptyset$ then we may take $\leq := \emptyset \subseteq \emptyset \times \emptyset$ again. As X does not contain any non-empty subsets A, there is nothing to prove. So from now on we assume $X \neq \emptyset$. We will prove the theorem by *zornification* that is we define the set of all well-ordered subsets of X

$$\mathcal{Z} \;:=\; \{ (A, \leq_A) \mid A \subseteq X, \leq_A \text{ is a well ordering on } A \}$$

First note that $\mathcal{Z}$ is non-empty: Since $X \neq \emptyset$ there is some $x \in X$ and we may take $A := \{ x \}$. There is precisely one ordering on A and this is a well-ordering, namely $\leq_A = (x, x)$. We now introduce a partial order $\leq$ on $\mathcal{Z}$: If $(A, \leq_A)$ and $(B, \leq_B) \in \mathcal{Z}$ then we take $(A, \leq_A) \leq (B, \leq_B)$ if $A \subseteq B$ and $\leq_A$ is the restriction of $\leq_B$ to A and B only contains no smaller elements than A. Formally that are the following three properties

(1) $A \subseteq B$

(2) $\forall\, a, b \in A \;:\; \big(a \leq_A b \iff a \leq_B b\big)$

(3) $\forall\, a \in A, \forall\, b \in B \setminus A \;:\; a \leq_B b$

It is clear that this truly is a partial order on $\mathcal{Z}$. In order to apply the lemma of Zorn we need to prove, that any chain $\mathcal{C} \subseteq \mathcal{Z}$ has an upper bound. Our candidate is $(U, \leq_U)$, where

$$U \;:=\; \bigcup \{ C \mid (C, \leq_C) \in \mathcal{C} \}$$

as a subset of X. And for any $u, v \in U$ we define the relation $\leq_U$ by taking

$$x \leq_U y \quad :\iff \quad \exists\, (C, \leq_C) \in \mathcal{C} \;:\; u, v \in C \text{ and } u \leq_C v$$

We will now prove the following: For any $u, v \in U$ and any $(A, \leq_A) \in \mathcal{C}$ such that $u, v \in A$ we have the equivalence

$$u \leq_U v \quad \iff \quad u \leq_A v$$

If $\neg(u \leq_U v)$ then there is no $(C, \leq_C) \in \mathcal{C}$ such that $u, v \in C$ and $u \leq_C v$. But as $u, v \in A$ this must mean $\neg(u \leq_A v)$. Conversely if $u \leq_U v$ then there is some $(C, \leq_C) \in \mathcal{C}$ such that $u, v \in C$ and $u \leq_C v$. That is we have $u, v \in A \cap C$. As $\mathcal{C}$ is a chain we either have $(A, \leq_A) \leq (C, \leq_C)$ other the other way around. In this case we have $u, v \in A \subseteq C$ such that $u \leq_C v$ implies $u \leq_A v$ according to property (2). If conversely $(C, \leq_C) \leq (A, \leq_A)$ we still have $u, v \in C$ such that $u \leq_C v$ implies $u \leq_A v$ by property (2), as well.

Next we will verify that $\leq_U$ is a total order on U. If $u \in U$ then there is some $(C, \leq_C) \in \mathcal{C}$ such that $u \in C$. Thereby $u \leq_C u$ such that $u \leq_U u$ again. Now consider $u, v, w \in U$ such that $u \leq_U v$ and $v \leq_U w$. By construction this means that $u, v \in A$ for some $(A, \leq_A) \in \mathcal{C}$ and likewise $v, w \in B$ with $v \leq_B w$. As $\mathcal{C}$ is a chain we either have $(A, \leq_A) \leq (B, \leq_B)$ or the other way around. In this case we have $u \in A \subseteq B$ such that u, v and $w \in B$. Now $u \leq_A v$ implies $u \leq_B v$ and with $v \leq_B w$ this is $u \leq_B w$. Thereby $u \leq_U v$ again. And $(B, \leq_B) \leq (A, \leq_A)$ can be treated completely analogous. In particular for $u = w$ we have $u \leq_B v$ and $v \leq_B u$ imply $u = v$. So we also have the anti-symmetry $u \leq_U v$, $v \leq_U u \implies u = v$. To show that $\leq_U$ is total we finally pick up any $u, v \in U$. That is $u \in A$ and $v \in B$ for some $(A, \leq_A)$ and $(B, \leq_B) \in \mathcal{C}$. As $\mathcal{C}$ is a chain we may assume $(A, \leq_A) \leq (B, \leq_B)$ without loss on generality. Now $u \in A \subseteq B$ yields either $u \leq_B v$ or $v \leq_B u$. Accordingly we get $u \leq_U v$ or $v \leq_U u$ as needed.

In the next step we have to verify that $\leq_U$ is a well-ordering on U: That is we are given any non-empty subset $A \subseteq U$ and need to find a least element of this. Fix some $a \in A \subseteq U$ and take some $(C, \leq_C) \in \mathcal{C}$ such that $a \in C$. As $\leq_C$ is a well-ordering the set $A \cap C$ has a least element m. That is $m \in A \cap C$ and for any $b \in A \cap C$ we have $m \leq_C b$. If now $b \in A \subseteq U$ is any element in A, then there is some $(B, \leq_B) \in \mathcal{C}$ such that $b \in B$. We distinguish two cases: If $b \in C$ then $b \in A \cap C$ such that $m \leq_C b$ and thereby $m \leq_U b$. If $b \notin C$ then $b \in B \setminus C$. As $\mathcal{C}$ is totally ordered we have $(C, \leq_C) \leq (B, \leq_B)$ as the other relation would require $B \subseteq C$. Now note that $m \in C$ and $b \in B \setminus C$ imply $m \leq_B b$ by property (3). Again this is $m \leq_U b$. Thus A has a least element m.

By now we have $(U, \leq_U) \in \mathcal{Z}$ and we will show that for any $(A, \leq_A) \in \mathcal{C}$ we have $(A, \leq_A) \leq (U, \leq_U)$. First of all we have $A \subseteq U$ by construction of U. Also for any $a, b \in A$ we have seen $a \leq_A b \iff a \leq_U b$. So it remains to verify property (3): Consider any $a \in A$ and $b \in U \setminus A$, then we need to show $a \leq_U b$. But since $b \in U$ there is some $(B, \leq_B) \in \mathcal{C}$ such that $b \in B$. As $\mathcal{C}$ is a chain $(A, \leq_A)$ and $(B, \leq_B)$ are comparable. But $(B, \leq_B) \leq (A, \leq_A)$ cannot be due to $b \in B \setminus A$ we necessarily have $(A, \leq_A) \leq (B, \leq_B)$. From this we get $a \leq_B b$ which in turn is $a \leq_U b$. That is $(U, \leq_U)$ is an upper bound of $\mathcal{C}$.

By now we have proved that any chain $\mathcal{C} \subseteq \mathcal{Z}$ has an upper bound $(U, \leq_U)$. Thus by the lemma of Zorn (0.28) there is a maximal element $(M, \leq_M)$ in $\mathcal{Z}$. Suppose there was some $x \in X \setminus M$, then we would define $M' := M \cup \{ x \}$ and

$$\leq_{M'} \;:=\; \leq_M \;\cup \{ (m, x) \mid m \in M' \}$$

That is $\leq_{M'}$ is the order of M' that features $m \leq_{M'} x$ for any $m \in M$ and is just $\leq_M$ when restricted to M. By construction $(M', \leq_{M'})$ is a totally ordered set, such that $\leq_{M'}$ even is a well-ordering of M': If $A \subseteq M'$ then either $A \cap M \neq \emptyset$ or $A = \{ x \}$. In the first case the least element of $A \cap M$ is the least element of A, in the second case it is x. That is $(M', \leq_{M'}) \in \mathcal{Z}$ and $(M, \leq_M) \leq (M', \leq_{M'})$. But as $(M, \leq_M)$ is maximal, this means $M = M'$ which contradicts $x \in X \setminus M$. Thus we could not have chosen x in the first place, such that $X = M$. But therefore $\leq_M$ is a well ordering on X itself. □

Proof of (0.32):

(i) If X or $Y = \emptyset$, then there are neither functions $X \to Y$ nor functions $Y \to X$, as both would have to be subsets of $X \times Y = \emptyset$. Thus we have $X \neq \emptyset$ and $Y \neq \emptyset$. Now suppose $X \hookrightarrow Y$, that is we are given an injective function $f : X \hookrightarrow Y$. If we had $f(X) = Y$, then f would also be surjective, hence bijective, so $f^{-1} : Y \twoheadrightarrow X$ would already be the function we need. In case $B := f(X) \subset Y$ choose any $x_0 \in X$ and define $g : Y \to X$ by $g(y) := f^{-1}(y)$ for $y \in B$ and $g(y) := x_0$ for $y \in Y \setminus B$. Then $g(B) = f^{-1}(B) = X$, such that g is surjective.

Conversely if $Y \twoheadrightarrow X$ we are given a surjective function $g : Y \twoheadrightarrow X$. We define an equivalence relation on Y, by letting $y \sim y' :\Longleftrightarrow g(y) = g(y')$. Then $q : Y/\sim \to X : [y] \mapsto g(y)$ is well-defined and bijective: By definition $[y] = [y']$ is $y \sim y'$ which in turn is $g(y) = g(y')$. Therefore q is well-defined and injective. But it also is surjective: Given any $x \in X$ choose some $y \in Y$ with $g(y) = x$ - recall that g was assumed to be surjective. Then $q([y]) = g(y) = x$. But by the axiom of choice there is a set $B \subseteq Y$ such that the map $p : B \to Y/\sim : y \mapsto [y]$ is bijective, too. Therefore the map $qp : B \to X$ is bijective and hence $(qp)^{-1} : X \to B \subseteq Y$, as well. But this means, that $(qp)^{-1} : X \hookrightarrow Y$ is injective.

(ii) Let us take the set $\mathcal{Z} := \{ (A, f) \mid A \subseteq X, f : A \hookrightarrow Y \}$ of pairs of subsets $A \subseteq X$ and injective functions f from A into Y. As X and Y are non-empty, we may pick any two elements $x \in X$ and $y \in Y$ and define $A := \{ x \}$ and $f : A \to Y$ by $f(x) := y$. Then $(A, f) \in \mathcal{Z}$, such that this set is non-empty.

Also if (A, f) and $(B, g) \in \mathcal{Z}$, then we define a relation $\leq$ on $\mathcal{Z}$ by letting $(A, f) \leq (B, g)$ iff $A \subseteq B$ and $\forall\, a \in A : g(a) = f(a)$. Clearly $\leq$ is a partial order on $\mathcal{Z}$. Now consider any chain $(A_i, f_i) \subseteq \mathcal{Z}$ (where $i \in I$). Then we define

$$A := \bigcup_{i \in I} A_i$$

$$f : A \to Y : a \mapsto f_i(a) \text{ for any } i \in I \text{ with } a \in A_i$$

Let us check that f is well-defined: If $a \in A$ then there truly is some $i \in I$ with $a \in A_i$ by construction of A. And if $j \in I$ is any index with $a \in A_j$ then we have $A_i \subseteq A_j$ or $A_j \subseteq A_i$ as the chain is totally ordered. Then we also have $f_j(a) = f_i(a)$ or $f_i = f_j(a)$ by construction of $\leq$. But as $f_j(a) = f_i(a)$ it does not matter, which $j \in I$ with $a \in A_j$ we took. Also f is injective: Given any $a, b \in A$ with $f(a) = f(b)$, there are some $i, j \in I$ with $a \in A_i$ and $b \in A_j$. By interchanging we may assume $A_i \subseteq A_j$. Then, as also $a \in A_j$, we have $f(b) = f(a) = f_j(a) = f_i(a) = f(a)$. In particular $(A, f) \in \mathcal{Z}$ and $(A_i, f_i) \leq (A, f)$.

We have just argued, that any chain in $\mathcal{Z}$ has an upper bound such that we may invoke the lemma of Zorn (0.28) to find a maximal element (A^*, f^*) of $\mathcal{Z}$. We distinguish two cases: If $A^* = X$ then $f : X \hookrightarrow Y$ is injective itself. So let us deal with $A^* \subset X$ a proper subset. Suppose we had $f^*(A^*) \neq Y$, then there was some $y \in Y \setminus f^*(A^*)$. Also there is some $x \in X \setminus A^*$. Now take $B := A^* \cup \{ x \}$ and $g(b) := f^*(b)$ for $b \in A^*$ and $g(b) := y$ for $b = x$. Then $(A^*, f^*) < (B, g)$ in contradiction to the maximality of (A^*, f^*). From this contradiction we conclude $f^*(A^*) = Y$. Now, as $f^* : A^* \longleftrightarrow Y$ is bijective, we may take its inverse $Y \longleftrightarrow A^* \subseteq X$. This is the injective map $Y \hookrightarrow X$ we needed.

(iii) In case of (b) there is a bijective map $f : X \longleftrightarrow Y$. In particular $f : X \hookrightarrow Y$ is injective. But $f^{-1} : Y \hookrightarrow X$ is bijective (and hence injective), too, such that (a) follows immediately. If we start with (a) and need to prove (b) the story is a little more complicated:

By assumption there are some injective maps $f : X \hookrightarrow Y$ and $g : Y \hookrightarrow X$. Without loss of generality we may assume X and Y to be disjoint, if they are not, just look at $X' := \{1\} \times X$ and $Y' := \{2\} \times Y$ instead. For these sets it is clear, that $X' \cap Y' = \emptyset$ and that we have the obvious bijections $X \longleftrightarrow X' : x \mapsto (1, x)$ and $Y \longleftrightarrow Y' : y \mapsto (2, y)$. Thus the maps we would construct on X' and Y' can be transferred back to X and Y.

Let $Z := X \cup Y$ and remember: $X \cap Y = \emptyset$ by assumption. Starting with any $z \in Z$ we will define a sequence $(z_0, z_1, z_2, z_3, \dots)$ (that may or may not terminate) recursively. This sequence will always alternate, its elements will either be in $X \times Y \times X \times Y \times \dots$ or in $Y \times X \times Y \times X \times \dots$. We start with $z_0 := z$ and suppose we had already constructed $(z_0, \dots, z_n) \in Z^{n+1}$. Then we continue

- if $z_n \in f(X) \subseteq Y$, then we take $z_{n+1} := f^{-1}(z_n) \in X$
- if $z_n \in g(Y) \subseteq X$, then we take $z_{n+1} := g^{-1}(z_n) \in Y$
- if neither $z_n \in f(X)$ nor $z_n \in g(Y)$, then stop

We denote the chain generated by this algorithm, if we start with $z = z_0 \in Z$ will be denoted by $C(z)$. If $C(z)$ is finite, say $C(z) = (z_0, \dots, z_n)$, then we denote $\ell(z) := n \in \mathbb{N}$. Else, if the algorithm does not terminate at all, we say $\ell(z) := \infty$. Clearly this algorithm subdivides X in three separate parts:

$$\begin{aligned} X_1 &:= \{ x \in X \mid \ell(x) \in 1 + 2\mathbb{Z} \} \\ X_2 &:= \{ x \in X \mid \ell(x) \in 2\mathbb{Z} \} \\ X_\infty &:= \{ x \in X \mid \ell(x) = \infty \} \end{aligned}$$

Note that $x \in X_2$ means that the chain $C(x) = (z_0 = x, z_1, \dots, z_n)$ stops with some $z_n \in X \setminus g(Y)$. This can already happen at $n = 0$, namely if $x \notin g(Y)$. And likewise $x \in X_1$ means that $C(x)$ stops with some $z_n \in Y \setminus f(X)$. In particular $n \geq 1$ and hence $x \in g(Y)$. In exactly the same fashion we define the sets Y_1, Y_2 and $Y_\infty \subseteq Y$. By construction X and Y are the disjoint unions of these sets respectively

$$\begin{aligned} X &= X_1 \cup X_2 \cup X_\infty \\ Y &= Y_1 \cup Y_2 \cup Y_\infty \end{aligned}$$

The idea now lies in proving $f(X_2) = Y_1$ and $g(Y_2) = X_1$ and $f(X_\infty) = Y_\infty$. Then $X_2 \longleftrightarrow Y_1$ under f, $Y_2 \longleftrightarrow X_1$ under g and $X_\infty \longleftrightarrow Y_\infty$ under f, as these maps are injective. Thereby we can glue together a bijection $h : X \to Y$ by taking $h(x) := f(x)$ if $x \in X_2 \cap X_\infty$ and $h(x) := g^{-1}(x)$ for $x \in X_1$. And this is precisely what we need in (b).

So it remains to prove $f(X_2) = Y_1$ in a first step: Let us start with any $x \in X_2$, that is $C(x) = (x, y_1, x_2, \dots, y_n)$, where n is even (maybe 0). We need to show $y := f(x) \in Y_1$. So let the algorithm start in y: In the first step we have $y = \in f(x) \in f(X)$ and hence get $z_1 = f^{-1}(y) = x$.

That is the next element in the chain of y is x and from there on we know what will happen: $C(y) = (y, x, y_1, x_2, \dots, y_n)$. In particular $\ell(y) = n+1$ is odd and thereby $f(x) = y \in Y_1$. Conversely we start with some $y \in Y_1$ and need to find some $x \in X_2$ such that $f(x) = y$. As $y \in Y_1$ the chain that starts in y is of the form $C(y) = (y, x_1, y_2, \dots, x_n)$, where n is odd and in particular $n \geq 1$. That is, we have x_1, so what is it? By construction this means $y \in f(X)$ and $x_1 := f^{-1}(y)$. That is $y = f(x_1)$. Clearly $C(x_1) = (x_1, y_2, \dots, x_n)$ such that $\ell(x_1) = n-1$ is even. That is $x_1 \in X_2$ and thereby we have found an $x := x_1 \in X_2$ such that $y = f(x)$.

Of course we find $g(Y_2) = X_1$ in exactly the same manner. So it remains to prove $f(X_\infty) = Y_\infty$, but this is much the same, too: Consider any $x \in X_\infty$ and let $y := f(x)$. Then $C(y) = (y, x, \dots)$, as in the first step we have $y \in f(X)$ and thereby $z_1 = f^{-1}(y) = x$. Thus $C(y)$ does not terminate and hence $y \in Y_\infty$. Conversely again, given $y \in Y_\infty$ the chain $C(y) = (y, x_1, y_2, x_3, y_4, \dots)$ does not terminate. In particular x_1 is given by $x_1 = f^{-1}(y)$ and hence $y = f(x_1)$. Again $C(x_1) = x_1, y_2, x_3, y_4, \dots)$ does not terminate, making $x_1 \in X_\infty$.

Altogether we have established the equalities $f(X_2) = Y_1$, $g(Y_2) = X_1$ and $f(X_\infty) = Y_\infty$ and as X resp. Y are the disjoint unions of these subsets we can glue together a bijection h, as described above.

(vi) Let us prove $|X| = |X|$ for any set X. In case $X = \emptyset$ the symbol $|X| = |X|$ is true, by definition. And if $X \neq \emptyset$ then the identity $x \mapsto x$ is a bijective map on X. Thus we have $|X| = |X|$ in this case, too.

Next we prove $|X| \leq |Y|$ or $|X| \leq |Y|$: If $X = \emptyset$ then $|X| \leq |Y|$ and if $Y = \emptyset$, then $|Y| \leq |X|$. It remains to regard the case when both, X and Y, are non-empty. Then by assumption we have $X \hookrightarrow Y$ or $Y \hookrightarrow X$ by (ii) which is $|X| \leq |Y|$ or $|Y| \leq |X|$ respectively. Thus one of the two is always satisfied.

Now to $|X| \leq |Y|$ and $|Y| \leq |Z|$ implies $|X| \leq |Z|$: If we have $X = \emptyset$ then $|X| \leq |Z|$ is satisfied trivially. And if $Y = \emptyset$ then $X \hookrightarrow Y$ is false (there are no functions that target Y) such that we also have $X = \emptyset$, as well. And in this case $|X| \leq |Z|$ is satisfied trivially, again. So now suppose that both, X and Y, are non-empty. Then $|X| \leq |Y|$ turns into $f : X \hookrightarrow Y$ and $|Y| \leq |Z|$ turns into $g : Y \hookrightarrow Z$. for some injective f, g. Then the composition $gf : X \hookrightarrow Z$ also is injective, such that $|X| \leq |Z|$ is satisfied.

It remains to prove the anti-symmetry $|X| \leq |Y|$ and $|Y| \leq |X|$ implies $|X| = |Y|$: If $X = \emptyset$ then $|Y| \leq |X|$ implies $Y = \emptyset$, as above. In the same manner if $X = \emptyset$ then $|X| \leq |Y|$ implies $X = \emptyset$. But if $X = \emptyset = Y$, then $|X| = |Y|$ is satified trivially. So let us now assume X and Y to ne non-empty. Then $|X| \leq |Y|$ turns into $X \hookrightarrow Y$ and $|Y| \leq |X|$ turns into $Y \hookrightarrow X$. But then by (iii) we have just seen $X \longleftrightarrow Y$ which yields $|X| = |Y|$.

□

Proof of (0.35):

(i) In this easy case we are able to provide a bijective map s directly: That is we define $s : \mathbb{N} \to \mathbb{Z}$ and $\bar{s} : \mathbb{Z} \to \mathbb{N}$ and will prove that $\bar{s} = s^{-1}$ is the inverse map. In particular s is bijective and therefore $|\mathbb{N}| = |\mathbb{Z}|$. The following maps will do the trick

$$s \,:\, \mathbb{N} \to \mathbb{Z} \,:\, n \mapsto \begin{cases} n/2 \text{ if } n \text{ is even} \\ -(n+1)/2 \text{ if } n \text{ is odd} \end{cases}$$

$$\bar{s} \,:\, \mathbb{Z} \to \mathbb{N} \,:\, k \mapsto \begin{cases} 2k \text{ if } n \geq 0 \\ -(2k+1) \text{ if } k < 0 \end{cases}$$

Note that n is *even*, iff it is of the form $n = 2m$ for some $m \in \mathbb{N}$ and n is *odd* iff $n = 2m+1$ for some $m \in \mathbb{N}$. As we argued above, it suffices to show that $\bar{s} = s^{-1}$, we begin with $\bar{s}s(n) = n$ for any $n \in \mathbb{N}$: If n is even then $s(n) = n/2 \geq 0$ and thereby $\bar{s}s(n) = 2 \cdot (n/2) = n$. If n is odd, say $n = 2m+1$ then $s(n) = -(n+1)/2 = -(m+1) < 0$ and thereby $\bar{s}s(n) = -2k-1$ for $k = -(m+1)$. This is $2(m+1)-1 = 2m+1 = n$. Thus in both cases we have $\bar{s}s(n) = n$. We also have to prove $s\bar{s}(k) = k$ for any $k \in \mathbb{Z}$. For $k \geq 0$ we have $s\bar{s}(k) = s(2k) = 2k/2 = k$. Now let $k < 0$, say $k = -(m+1)$ where $m \in \mathbb{N}$, then we have $\bar{s}(k) = -2k-1 = 2(m+1)-1 = 2m+1$, which is an odd number and therefore $s\bar{s}(k) = -(2m+1+1)/2 = -(m+1) = k$. Again we have $s\bar{s}(k) = k$ in both cases and thereby $\bar{s} = s^{-1}$.

(ii) Let us split $\mathbb{N} \times \mathbb{N}$ into a sequence of finite sets: As any $(k,l) \in \mathbb{N}^2$ features finite k, l it is contained in a set of the form $B_n := \{\, (k,l) \in \mathbb{N}^2 \mid k \leq n, l \leq n \,\}$ for some $n \in \mathbb{N}$. And B_n is finite, as it contains exactly $(n+1)^2$ elements. Not let $A_0 := \{\, (0,0) \,\}$ and for any $n \geq 1$:

$$A_n \;:=\; B_n \setminus B_{n-1}$$

That is $A_1 = \{\, (0,1),(1,1),(1,0) \,\}$ and $A_2 = \{\, (0,2),(1,2),(2,2),(2,1),(2,0) \,\}$ and so on. In general $A_n = \{\, (k,n) \mid k \in 0 \ldots n \,\} \cup \{\, (n,k) \mid k \in 0 \ldots n \,\}$. That is

$$\#A_n \;=\; \#B_n - \#B_{n-1} \;=\; (n+1)^2 - n^2 \;=\; 2n+1$$

In particular we have $0 \ldots 2n \longleftrightarrow A_n$, that is we can enumerate the elements of A_n using $2n+1$ indices. Luckily $\mathbb{N}$ has space for infinitely many indices. Let $I_0 := \{0\}$ and for any $1 \leq n \in \mathbb{N}$ let I_n be the index set

$$I_n \;:=\; \left\{\, i \in \mathbb{N} \mid n^2 < i \leq (n+1)^2 \,\right\}$$

That is $\#I_n = (n+1)^2 - n^2 = \#A_n$ such that there is a bijection $b_n : I_n \longleftrightarrow A_n$. By construction it is clear, that the I_n for a partition of $\mathbb{N}$ and the A_n form a partition of $\mathbb{N}^2$. Hence we find a bijection between $\mathbb{N}$ and $\mathbb{N}^2$ by mapping the elements of I_n to A_n

$$\mathbb{N} \;=\; \bigcup_{n \in \mathbb{N}} I_n \;\longleftrightarrow\; \bigcup_{n \in \mathbb{N}} A_n \;=\; \mathbb{N}^2$$

(iii) For one it is clear, that $\mathbb{N} \hookrightarrow \mathbb{Q} : n \mapsto n/1$ is an injective map. Thus by Bernstein's equivalence theorem (0.32.(iii)) it suffices to find another surjective map $\mathbb{N} \twoheadrightarrow \mathbb{Q}$. We set out to construct such a map. Clearly

$$p \;:\; \mathbb{N} \times \mathbb{N} \;\twoheadrightarrow\; \left\{\, \frac{a}{b} \in \mathbb{Q} \;\middle|\; \frac{a}{b} \geq 0 \,\right\} \;:\; (a,b) \mapsto \frac{a}{b+1}$$

is surjective, as any $c/d \in \mathbb{Q}$ can be written as a/b for some $b \geq 1$: As $d \neq 0$ we either have $d \geq 1$ or $d \leq -1$ and in the latter case we can take $a := -c$ and $b := -d$. We then find another surjective map onto the negative rationals, in a similar fashion

$$q \ : \ \mathbb{N} \times \mathbb{N} \ \twoheadrightarrow \ \left\{ \frac{a}{b} \in \mathbb{Q} \ \middle| \ \frac{a}{b} \leq 0 \right\} \ : \ (a,b) \ \mapsto \ -\frac{a}{b+1}$$

Let us pick up any $t : \mathbb{N} \longleftrightarrow \mathbb{N} \times \mathbb{N}$, one of those bijective maps, that exist, according to (ii). Then we can present a map from $\mathbb{Z}$ to $\mathbb{Q}$ by letting

$$\mathbb{Z} \ \to \ \mathbb{Q} \ : \ k \ \mapsto \begin{cases} pt(k) \text{ if } k \geq 0 \\ qt(-k-1) \text{ if } k < 0 \end{cases}$$

Let us prove that this is surjective: Given any $a/b \in \mathbb{Q}$ we may assume $b \geq 1$. We then check whether $a/b \geq 0$: If this is the case, we have $p(a, b-1) = a/b$. And as t is bijective there is some $k \in \mathbb{N}$ with $t(k) = (a, b-1)$. Therefore $k \mapsto a/b$. Otherwise, if $a/b < 0$ $a < 0$ such that $-a \in \mathbb{N}$ and $q(-a, b-1) = a/b$. Again, as t is bijective, there is some $n \geq 1$ with $t(n-1) = (-a, b-1)$. And thereby we get $-n \mapsto qt(n-1) = q(-a, b-1) = a/b$. Thus this map reaches any $a/b \in \mathbb{Q}$ and thereby is surjective. But by (i) we can use this to get our surjective map

$$\mathbb{N} \ \longleftrightarrow \ \mathbb{Z} \ \twoheadrightarrow \ \mathbb{Q}$$

(iv) As Ω is countable, we have $|\Omega| \leq |\mathbb{N}|$. That is $\Omega \hookrightarrow \mathbb{N}$ or equivalently - by (0.32.(i)) - $\mathbb{N} \twoheadrightarrow \Omega$. That is there is a surjective map of the form $\omega : \mathbb{N} \twoheadrightarrow \Omega$. Also for any $i \in \Omega$ the set A_i is countable. If $A_i = \emptyset$, then we may ignore it, else there is a surjective mapping $\alpha(i) : \mathbb{N} \twoheadrightarrow A_i$.

By (ii) there also is a bijective map $\beta : \mathbb{N} \longleftrightarrow \mathbb{N} \times \mathbb{N}$. For any $n \in \mathbb{N}$ let us denote $\beta(n) = (\beta_1(n), \beta_2(n))$. We use all this to define a map of the form

$$s \ : \ \mathbb{N} \to \bigcup_{i \in \Omega} A_i \ : \ n \mapsto \alpha\big(\omega(\beta_1(n))\big)(\beta_2(n))$$

That is the first entry of $\beta(n)$ is used to choose the set A_i to pick from and the second entry of $\beta(n)$ is used to pick an element. Therefore s is surjective: Consider any $a_i \in A_i$, as $i \in \Omega$ there is some $k \in \mathbb{N}$ with $i = \omega(k)$. And as $a_i \in A_i$ there is some $l \in \mathbb{N}$ with $a_i = \alpha(i)(l)$. Now choose $n \in \mathbb{N}$ with $\beta(n) = (k, l)$, that is $i = \omega(k) = \omega(\beta_1(n))$ and $a_i = \alpha(i)(l) = \alpha(i)\beta_2(n))$. Together this is $a_i = s(n)$ and as we can do this for any $i \in \Omega$ and any $a_i \in A_i$ the map s is surjective. But $\mathbb{N} \twoheadrightarrow \bigcup_i A_i$ means, that the union is countable, again.

(v) The map $X \hookrightarrow \mathcal{P}(X) : x \mapsto \{ x \}$ obviously is injective, such that $|X| \leq |\mathcal{P}(X)|$. And if we consider any function $f : X \to \mathcal{P}(X)$, then we will show that f cannot be surjective: As $f(x)$ is a subset of X it makes sense, to define the following subset

$$R \ := \ \{ x \in X \mid x \notin f(x) \} \ \in \ \mathcal{P}(X)$$

Suppose there was some $r \in X$ with $f(r) = R$, then we raise the question: Is $r \in R$? Suppose we had $r \in R = f(r)$ then by construction of R we had $r \notin R$, a contradiction. Suppose we had $r \notin R$, then $r \notin f(r)$ was false and hence $r \in f(r) = R$, a contradicition, again. Either way the coin lands, we arrive at a contradiction and this means there is no $r \in X$ with $f(r) = R$. In other words, f is *not* surjective. Thus we cannot have $|X| = |\mathcal{P}(X)|$ and this is summarized in $|X| < |\mathcal{P}(X)|$.

□

Proof of (0.36):
Abbreviate $A := \bigcup \mathcal{A}$ and $B := \bigcup \mathcal{B}$ the grand union, respectively. If $a \in A$ then there is some $i \in I$ with $a \in A_i$. And as the A_i are pairwise distinct, this i even is uniquely determined. Also there is a bijective map $\mathfrak{a}_i : A_i \longleftrightarrow B_{\beta(i)}$ by assumption. Thus we get a well-defined map, by letting

$$\alpha \ : \ A \ \to \ B \ : \ a \ \mapsto \ \alpha_i(a) \text{ where } a \in A_i$$

This map is injective: Suppose $\alpha(a_i) = \alpha(a_j)$ where $a_i \in A_i$ and $a_j \in \forall_j$. By construction this means $\alpha_i(a_i) = \alpha_j(a_j) \in B_k$ for some $k \in K$. By construction of α_i this k is $k = \beta(i)$ and likewise $k = \beta(j)$. But as β is injective, $\beta(i) = \beta(j)$ implies $i = j$. But α_i is injective, as well and hence $\alpha_i(a_i) = \alpha_i(a_j)$ implies $a_i = a_j$. But α also is surjective: Given any $b \in B$ there is some (uniquely determined) $k \in K$, such that $b \in B_k$. Let $i := \beta^{-1}(k)$ and $a := \alpha_i^{-1}(b)$, then $a \in A_i$ and thereby $\alpha(a) = \alpha_i(a) = b$ is clear. That is α is bijective and hence we gain the equality of the cardinalities. □

Proof of (0.38):

(i) For a set $\mathcal{P} \subseteq \mathcal{P}(X)$ of subsets of X let us abbreviate the following properties: (1) $\mathcal{P} \neq \emptyset$, (2) any $P \in \mathcal{P}$ is countably infinite and (3) for any $P, Q \in \mathcal{P}$ with $P \neq Q$ we have $P \cap Q = \emptyset$. Then we define the following set:

$$\mathcal{Z} \ := \ \{ \mathcal{P} \subseteq \mathcal{P}(X) \mid \text{(1), (2) and (3)} \}$$

As X is infinite, we have $\mathbb{N} \hookrightarrow X$ and thereby X contains some countably infinite subset $P := \{ x_n \mid n \in \mathbb{N} \} \subseteq X$. Thereby $\mathcal{P} := \{ P \}$ satisfies (1) to (3) and thereby $\mathcal{Z} \neq \emptyset$. Clearly $\mathcal{Z}$ is partially ordered under inclusion "$\subseteq$". And if $(\mathcal{C}_i) \subseteq \mathcal{Z}$ is a chain in $\mathcal{Z}$ (where $i \in I$), then the union $\bigcup_i \mathcal{C}_i$ is an element of $\mathcal{Z}$ again: Properties (1) and (2) are obvious and for (3) we consider any $P \in \mathcal{C}_i$ and $Q \in \mathcal{C}_j$. As the $\mathcal{C}_i$ form a chain, we may assume $\mathcal{C}_i \subseteq \mathcal{C}_j$ without loss of generality. Then $P \in \mathcal{C}_j$ is true, as well. Thus if $P \neq Q$ then $P \cap Q = \emptyset$ by (3) of $\mathcal{C}_j$ and hence we have (3) for $\bigcup_i \mathcal{C}_i$ too. Thus by the lemma of Zorn (0.28) or remark (2.1.(ix)) there is a maximal element $\mathcal{M} \in \mathbb{Z}$. We now claim, that

$$B \ = \ X \setminus \bigcup \mathcal{M}$$

is a finite set: Suppose not, that is B is infinite and thereby there is some $\mathbb{N} \hookrightarrow B$, in other words $A = \{ x_n \mid n \in \mathbb{N} \} \subseteq B$. Thereby $A \subseteq X$ and thus $\mathcal{M} \cup \{ A \}$ satisfies (1) to (3) again. As before (1) and (3) are clear and for (3) we regard any $P, Q \in \mathcal{M} \cup \{ A \}$ with $P \neq Q$. If both $P, Q \in \mathcal{M}$, then $P \cap Q = \emptyset$ by (3) of $\mathcal{M}$, so we may assume $P \in \mathcal{M}$ and $Q = A$. Then $P \in \mathcal{M}$ implies $P \subseteq \bigcup \mathcal{M} = X \setminus B$ and then $Q = A \subseteq B$ yields $P \cap Q = \emptyset$. Thus we have $\mathcal{M} \subset \mathcal{M} \cup \{ A \} \in \mathcal{Z}$ in contradiction to the maximality of $\mathcal{M}$ and this means B must be finite. Let us now construct a suitable $\mathcal{P}$ out of $\mathcal{M}$ and B: Choose any $Q \in \mathcal{M}$ and replace Q with $Q \cup B$, that is

$$\mathcal{P} \;:=\; \big(\mathcal{M} \setminus \{\, Q \,\}\big) \cup \{\, Q \cup B \,\}$$

Then $Q \cup B$ clearly is countable again, so $\mathcal{P}$ satisfies (2). Also $\mathcal{P}$ satisfies (3), that is the elements of $\mathcal{P}$ are pairwise disjoint and finally X is the grand union of $\mathcal{P}$, as $\bigcup \mathcal{P} = \bigcup \mathcal{M} \cup B = (X \setminus B) \cup B = X$. Thus $\mathcal{P}$ is a partition of X consisting of countable sets, only.

(ii) By (i) there is a partition $\mathcal{P} = \{\, P_i \mid i \in I \,\}$ of X, such that any P_i is countably infinite. Let $P_i := \{\, x_{i,k} \mid k \in \mathbb{N} \,\}$, the trick is to decompose $\mathbb{N}$ into the subsets $k - 1 + n\mathbb{N} \subseteq \mathbb{N}$. For $k = 1$ this is $n\mathbb{N} = \{\, nk \mid k \in \mathbb{N} \,\}$ up to $n - 1 + n\mathbb{N} = \{\, (n-1) + nk \mid k \in \mathbb{N} \,\}$. This partition can be used to partition P_i into n distinct subsets

$$A_{i,j} \;:=\; \{\, x_{i,k} \mid k \in (j-1) + n\mathbb{N} \,\}$$

The sets $\{\, A_{i,1}, \ldots, A_{i,n} \,\}$ inherit being a partition of P_i from the sets $\{\, n\mathbb{N}, \ldots, (n-1) + n\mathbb{N} \,\}$, that partition $\mathbb{N}$. Also any $A_{i,j}$ is countably infinite by construction and thereby $|P_i| = |A_{i,j}|$ under the bijection $x_{i,k} \mapsto x_{i,(j-1)+nk}$. And from this it is clear that $A_1, \ldots, A_n$ partition X, where

$$A_j \;:=\; \bigcup_{i \in I} A_{i,j}$$

That is we have properties (1) and (2) for these sets. The third property $|X| = |A_j|$ is inherited from $|P_i| = |A_{i,j}|$ using proposition (0.36), as both unions run over $i \in I$.

(iii) Let us start with (a) $\implies$ (b): As X is infinite there is $\mathbb{N} \hookrightarrow X$ such that X has a countably infinite subset $C = \{\, x_n \mid n \in \mathbb{N} \,\} \subseteq X$. And if $m := \#F \in \mathbb{N}$, then we write F in the form $F = \{\, f_0, \ldots, f_{m-1} \,\}$. Then we are able to define a map, that obviously is bijective

$$X \longleftrightarrow X \cup F \;:\; x \mapsto \begin{cases} f_k \text{ if } x = x_k \text{ where } k < m \\ x_{k-m} \text{ if } x = x_k \text{ where } k \geq m \\ x \text{ if } x \notin C \end{cases}$$

Conversely for (b) $\implies$ (a) we use proof by contradiction: Suppose X *was* finite, say $n := \#X$ and $X = \{\, x_1, \ldots, x_n \,\}$. Then we pick up any set F that contains an element, not contained in X before, e.g. $F := \{\, X \,\}$. Then $F \cap X \neq \emptyset$ would mean $X \in X$ which is not allowed, for sets. Then $X \cup F$ would contain $n+1$ elements, as we get a bijection $1 \ldots (n+1) \to X$ by $k \mapsto x_k$ and $n+1 \mapsto X$. Thus (b) was false, too.

- For (c) $\implies$ (a) proof by contradiction works, as well: Again suppose X *was* finite. Then we could choose $F := X$ and thereby get $X \setminus F = \emptyset$. Yet $X \neq \emptyset$ by assumption and thereby $|X|$ and $|X \setminus F|$ are not the same. Conversely for (a) $\implies$ (c) we use induction on the number $n := \#(X \cap F)$ of elements in $X \cap F$. For $n = 0$ we have $X \cap F = \emptyset$ and thereby $X \setminus F = X \setminus (X \cap F) = X \setminus \emptyset = X$. In particular $|X| = |X \setminus F|$. Now for the induction step $n \geq 1$ we consider $X \cap F = \{\, f_1, \ldots, f_n \,\}$. By induction hypothesis, we have $X \longleftrightarrow X' := X \setminus \{\, f_2, \ldots, f_n \,\}$. Then $X \setminus F = X \setminus \{\, f_1, \ldots, f_n \,\} = X' \setminus \{\, f_1 \,\}$. And as X' is infinite (X is infinite and has the same cardinality) there is a countably infinite set $C \subseteq X'$. Without loss of generality we may assume $f_1 \notin C$, if we had $f_1 \in C$ then we could simply take to $C \setminus \{\, f_1 \,\}$, which countably infinite again

- just like $\mathbb{N} \setminus \{0\}$. Let $C = \{ x_k \mid k \in \mathbb{N} \} \subseteq X'$ where $f_1 \notin C$. Using this we can define a map, that obviously is bijective

$$X' \longleftrightarrow X' \setminus \{ f_1 \} \; : \; x \mapsto \begin{cases} x_0 \text{ if } x = f_1 \\ x_{k+1} \text{ if } x = x_k \\ x \text{ if } x \notin C, x \neq f_1 \end{cases}$$

Then we get $X \longleftrightarrow X' \longleftrightarrow X' \setminus \{ f_1 \} = X \setminus \{ f_1, \ldots, f_n \} = X \setminus F$. So if we compare X from the left hand side to $X \setminus F$ from the right hand side, we see $X \longleftrightarrow X \setminus F$ which is $|X| = |X \setminus F|$.

- The direction (a) $\implies$ (b) is surprisingly easy: Let us first regard the case $A = X$ and note that we can realize $X \sqcup X$ as $X_1 \cup X_2$ where $X_1 := \{ 1 \} \times X$ and $X_2 := \{ 2 \} \times X$. Next we use (ii) to get a partition $X = A \cup B$ of the infinite set X where $|X| = |A| = |B|$. That is there are bijective maps $f : A \longleftrightarrow X$ and $g : B \longleftrightarrow X$. These can be used to get a bijection

$$X = A \cup B \longleftrightarrow X \sqcup X \; : \; x \mapsto \begin{cases} (1, f(x)) \text{ if } x \in A \\ (2, g(x)) \text{ if } x \in B \end{cases}$$

Now for a general subset $A \subseteq X$ it is clear, that there is an injection of the form $A \sqcup X \hookrightarrow X \sqcup X$ by taking $(A, a) \mapsto (1, a) \in X_1$ and $(X, x) \mapsto (2, x) \in X_2$. Conversely there is an obvious injection of the form $X \hookrightarrow A \sqcup X$ given by $x \mapsto (X, x)$. Combining these, we get

$$A \sqcup X \hookrightarrow X \sqcup X \longleftrightarrow X \hookrightarrow A \sqcup X$$

And from $A \sqcup X \hookrightarrow X$ and $X \hookrightarrow A \sqcup X$ we conclude $A \sqcup X \longleftrightarrow X$ using Bernstein's equivalence theorem (0.32.(iii)). Conversely, for (d) $\implies$ (a) we assume X was finite, say $\#X = n$. Then $X \sqcup X$ is two copies of X and hence a finite set with $\#(X \sqcup X) = 2n$. As $n < 2n$ for $n \geq 1$ there can be no bijection between X and $X \sqcup X$, in contradiction to (d).

(iv) The only hard part is (a) $\implies$ (b) so let's get over it: We aim for a zornification, so let us define the following set, consisting of subsets $A \subseteq X$ equipped with a bijection $\beta : A \longleftrightarrow A \times A$

$$\mathcal{Z} \; := \; \{ (A, \beta) \mid A \subseteq X, \; \beta : A \longleftrightarrow A \times A \}$$

This set is non-empty: As X is infinite there is countably infinite subset $\mathbb{N} \longleftrightarrow A \subseteq X$. And as $\mathbb{N} \longleftrightarrow \mathbb{N} \times \mathbb{N}$ by (0.35.(ii)) this installs a bijection $\beta : A \longleftrightarrow A \times A$. Thus $(A, \beta) \in \mathcal{Z}$ such that $\mathcal{Z}$ is non-empty, it even contains some (A, β) with infinite set A. This set is partially ordered under the relation $(A, \alpha) \leq (B, \beta)$ iff $A \subseteq B$ and for any $a \in A$ we get $\alpha(a) = \beta(a)$. Now if $(A_i, \beta_i) \subseteq \mathcal{Z}$ is a chain in $\mathcal{Z}$ then we can take

$$A := \bigcup_{i \in I} A_i \quad \text{and} \quad \beta(a) := \beta_i(a) \text{ for any } i \in I \text{ with } a \in A_i$$

This is well-defined, as whenever $(A_i, \beta_i) \leq (A_j, \beta_j)$ and $a \in A_i$ then the functions $\beta_j(a) = \beta_i(a)$ agree by construction. And if $\beta(a) = \beta(b)$ for some $a \in A_i$ and $b \in A_j$ then we may assume $A_i \subseteq A_j$ and thereby $a \in A_j$. Then $\beta_j(a) = \beta_i(a) = \beta(a) = \beta(b) = \beta_j(b)$ implies $a = b$, as β_j is

injective. Given any $(a,b) \in A \times A$ we have $a \in A_i$ and $b \in A_j$ again. Again we assume $A_i \subseteq A_j$ and thereby $a \in A_j$ and find $\beta : \beta_j^{-1}(a,b) \mapsto (a,b)$, which also is the surjectivity of β. Altogether $(A,\beta) \in \mathcal{Z}$ is an upper bound of the chain (A_i,β_i). Thus by the lemma of Zorn (0.28), there is a maximal element $(M,\beta) \in \mathcal{Z}$. As we have seen above, that M is an infinite set, here.

Now that we've got a maximal element (M,β) let us regard $B := X \setminus M$. In the next step we will prove that $|B| < |M|$. Suppose there was some injective map $M \hookrightarrow B$, that is $\mu : M \longleftrightarrow A \subseteq B$ maps M onto a subset A of B bijectively. Note that $M \cap A = \emptyset$ are disjoint, as $M \subseteq X \setminus B$ and $A \subseteq B$. We now split $(M \cup A) \times (M \cup A)$ into 4 separate parts

	M	A
M	$M \times M$	$M \times A$
A	$A \times M$	$A \times A$

And we use (ii) for $n = 3$ to split A into 3 separate copies $A = A_1 \cup A_2 \cup A_3$. For any $i \in 1 \ldots 3$ let $\alpha_i : A_i \longleftrightarrow A$ be the bijective maps, we've got. Then we can build up the chain of bijections

$$A_1 \longleftrightarrow A \longleftrightarrow M \longleftrightarrow M \times M \longleftrightarrow A \times A$$

that is $(\mu \times \mu)\beta\mu^{-1}\alpha_1 : A_1 \longleftrightarrow A \times A$. In much the same way we find the bijection $(\mathbb{1}_M \times \mu)\beta\mu^{-1}\alpha_2$ of the sets $A_2 \longleftrightarrow M \times A$ and $(\mu \times \mathbb{1}_M)\beta\mu^{-1}\alpha_3$ of the sets $A_3 \longleftrightarrow A \times M$ by composing

$$A_2 \longleftrightarrow A \longleftrightarrow M \longleftrightarrow M \times M \longleftrightarrow M \times A$$

$$A_3 \longleftrightarrow A \longleftrightarrow M \longleftrightarrow M \times M \longleftrightarrow A \times M$$

We that is we can assign the 4 parts of $M \cup A = M \cup A_1 \cup A_2 \cup A_3$ to the 4 parts of $(M \cup A) \times (M \cup A)$. Using (0.36) this can be patched together into a single bijection

$$\begin{aligned} M \cup A &= M \cup A_1 \cup A_2 \cup A_3 \\ &\longleftrightarrow (M \times M) \cup (A \times A) \cup (M \times A) \cup (A \times M) \\ &= (M \cup A) \times (M \cup A) \end{aligned}$$

Note that the first patch $M \longleftrightarrow M \times M$ is β and hence we have found an extension $(M \cup A, \overline{\beta})$ of (M,β). But this is in contradiction to the maximality of (M,β) and hence could not have been the case. That is we have to discard the assumption $|M| \leq |B|$. As comparing cardinalities is a total order, by (0.32.(ii)), we conclude $|B| < |M|$. That is we can inject $\lambda : B \longleftrightarrow L \subseteq M$ onto some subset L of M. And thereby, by the (d) part of (iii) we get

$$X = B \cup M \longleftrightarrow L \sqcup M \longleftrightarrow M$$

That is we have a bijection $\xi : M \longleftrightarrow X$ and this can be used to compose the bijection $(\xi \times \xi)\mu\xi^{-1}$ of the sets $X \longleftrightarrow X \times X$. That is we compose the chain

$$X \longleftrightarrow M \longleftrightarrow M \times M \longleftrightarrow X \times X$$

- The other implications are easy: For (b) $\implies$ (d) we use induction on n: The case $n = 1$ is obvious, as $\mathbb{1} : X \longleftrightarrow X = X^1$ is a bijection. So by induction hypothesis there is a bijective map $\delta : X^n \longleftrightarrow X$. And by hypothesis (b) there also is a bijection $\beta : X^2 \longleftrightarrow X$. As also $\alpha : X^{n+1} \longleftrightarrow X^n \times X$ under $(x_1, \ldots, x_{n+1}) \mapsto ((x_1, \ldots, x_n), x_{n+1})$ we can compose these maps to find a bijection

$$X^{n+1} \longleftrightarrow X^n \times X \longleftrightarrow X \longleftrightarrow X$$

given by $\beta(\delta \times \mathbb{1}_X)\alpha : X^{n+1} \longleftrightarrow X$. This is the induction step and thereby (d). Now (d) $\implies$ (c) is trivial, by taking $x = 2$. It remains to return (c) $\implies$ (a): As always we suppose X was finite, by assumption we have $k := \#X \geq 2$. Then it is clear, that X^n is a finite set, too with $\#X^n = k^n$ elements. But as $n \geq 2$ and $k \geq 2$ we have $1 < k < k^{n-1}$ and thereby $k < k^n$. That is property (c), which reads as $k = |X| = |X^n| = k^n$, could not have been true.

- Let us now prove (a) $\implies$ (c): As X is infinite, there is a bijection $d_n : X \longleftrightarrow X^n$ for any $n \geq 1$, according to (iv). This can be used to construct a bijection of the following form

$$X \times \mathbb{N} \longleftrightarrow \bigcup_{n=1}^{\infty} X^n \; : \; (x, n) \mapsto d_n(x)$$

This map clearly is well-defined and injective: If $d_m(x) = d_n(y)$ then the lengths of the tuples $m = n$ must be equal and as d_n is injective, we also get $x = y$. Also if $(x_1, \ldots, x_n) \in X^n$ is any n-tuple, there is some $x \in X$ such that $d_n(x) = (x_1, \ldots, x_n)$, thus $(x, n) \mapsto (x_1, \ldots, x_n)$. That is the surjectivity of the above map. Also by (a) $\implies$ (b) there is a bijection $X \longleftrightarrow X \times \mathbb{N}$. Let us concatenate these bijections, then we read the claim from

$$X \longleftrightarrow X \times \mathbb{N} \longleftrightarrow \bigcup_{n=1}^{\infty} X^n$$

- Next in line is (c) $\implies$ (d): It is clear that $X \hookrightarrow \Omega(X) \setminus \{\emptyset\}$ defined by $x \mapsto \{x\}$ is an injective map. But we also get a surjective map of the following form

$$\bigcup_{n=1}^{\infty} X^n \twoheadrightarrow \Omega(X) \setminus \{\emptyset\} \; : \; (x_1, \ldots, x_n) \mapsto \{x_1, \ldots, x_n\}$$

That is we also have a surjection $X \longleftrightarrow \bigcup_n X^n \twoheadrightarrow \Omega(X) \setminus \{\emptyset\}$. By the Bernstein equivalence theorem (0.32.(iii)), this is $X \longleftrightarrow \Omega(X) \setminus \{\emptyset\}$. In particular $\Omega(X) \setminus \{\emptyset\}$ is an infinite set, as X is and by property (b) in (iii) this means

$$|X| \; = \; |\Omega(X) \setminus \{\emptyset\}| \; = \; |\big(\Omega(X) \setminus \{\emptyset\}\big) \cup \{\emptyset\}| \; = \; |\Omega(X)|$$

- Time to close the circle by proving (d) $\implies$ (a): Suppose X was finite, say $X = \{x_1, \ldots, x_n\}$. Then $\mathcal{O}(X) = \mathcal{P}(X)$, as any subset $A \subseteq X$, is finite, too. Then there is a bijection

$$\mathbb{B}^n \longleftrightarrow \mathcal{P}(X) \; : \; (b_1, \ldots, b_n) \mapsto \{x_k \mid b_k = 1\}$$

As $\mathbb{B} = \{0,1\}$ has two elements, we see $\#\mathbb{B}^n = 2^n$ where $n = \#X$ and thereby $\mathcal{P}(X) = 2^n$. But as $n < 2^n$ for any $n \geq 1$ we find that X and $\mathcal{P}(X) = \Omega(X)$ cannot have the same cardinality, in contradiction to (d). Alternatively, we could argue: As X is finite we get $\mathcal{O}(X) = \mathcal{P}(X)$. But by (0.35.(v)) we have $|X| < |\mathcal{P}(X)|$, which contradicts (d).

(vi) By (0.32.(ii)) we have $X \hookrightarrow Y$ or $Y \hookrightarrow X$. As $X \sqcup Y$ and $Y \sqcup X$ obviously have the same cardinality, we may assume $X \hookrightarrow Y$ without loss of generality, therefore we have to prove $|X \sqcup Y| = |Y|$. As $X \hookrightarrow Y$ there is a subset $U \subseteq Y$ with $X \longleftrightarrow U$. Then by property (d) in (iii) we have already have the claim $|X \sqcup Y| = |U \sqcup Y| = |Y|$.

- As above we may assume $X \subseteq Y$, and as $X \neq \emptyset$ we may fix any $x \in X$ and thereby get an injective map $Y \hookrightarrow X \times Y : y \mapsto (x,y)$. In particular $|Y| \leq |X \times Y|$. On the other hand, if $\iota : X \hookrightarrow Y$ is the injection, this induces $X \times Y \hookrightarrow Y \times Y : (x,y) \mapsto (\iota(x),y)$. But then by property (b) of of (iv) we get the second claim $|X \times Y| \leq |Y \times Y| = |Y|$, too.

(vii) First of all, we can omit any $i \in I$ with $A_i = \emptyset$, as these do not contribute to the union of the A_i. That is it suffices to regard $I_0 := \{\, i \in I \mid A_i \neq \emptyset \,\}$. As the remaining A_i are countable, they are of the form $A_i = \{\, a(i,n) \mid n \geq 1 \,\}$. Now define $A_n := \{\, a(i,n) \mid i \in I_0 \,\}$, then we get

$$A \;:=\; \bigcup_{i \in I} A_i \;=\; \bigcup_{n=1}^{\infty} A_n$$

As $|I| \leq |X|$ there is some injective map $I \hookrightarrow X$ and thereby I_0 corresponds $I_0 \longleftrightarrow X_0$ to a subset $X_0 \subseteq X$, that is X_0 is of the form $X_0 = \{\, x_i \mid i \in I_0 \,\}$. In particular, if we fix any $i_0 \in I_0$, we find a surjective map

$$X \;\twoheadrightarrow\; I_0 \;:\; x \mapsto \begin{cases} i \text{ if } x = x_i \\ i_0 \text{ if } x \notin X_0 \end{cases}$$

and this can be used to create another surjective map $X \twoheadrightarrow A_n : x_i \mapsto a(i,n)$. For any $n \geq 1$ let $X_n := X$ be a copy of X. Then it is clear that the following map is another surjection

$$\bigcup_{n=1}^{\infty} X^n \;\twoheadrightarrow\; \bigsqcup_{n=1}^{\infty} X_n \;:\; (x_1, \ldots, x_n) \mapsto (n, x_n)$$

By what we have argued above, any $X_n = X$ maps surjectively onto A_n and thereby we also have the following surjective map

$$\bigsqcup_{n=1}^{\infty} X_n \;\twoheadrightarrow\; \bigsqcup_{n=1}^{\infty} A_n \;:\; (n, x_n) \mapsto \begin{cases} a(i,n) \text{ if } x_n = x_i \\ a(i_0,n) \text{ if } x \notin X_0 \end{cases}$$

By property (c) in (v) we have a bijection between X and the union $\bigcup_n X_n$ so we can use this to compose the following chain of surjections, that proves the claim

$$X \;\longleftrightarrow\; \bigcup_{n=1}^{\infty} X^n \;\twoheadrightarrow\; \bigsqcup_{n=1}^{\infty} X_n \;\twoheadrightarrow\; \bigsqcup_{n=1}^{\infty} A_n \;\twoheadrightarrow\; \bigcup_{n=1}^{\infty} A_n \;=\; A$$

□

Proof of (9.4):

(i) Clearly for any $x \in X$ we have $x \sim x$, since $x = ex$. Also if $x \sim y$, say $y = gx$ for some $g \in G$, then $x = ex = (g^{-1}g)x = g^{-1}(gx) = g^{-1}y$ such that we also have $y \sim x$. And if also $y \sim z$, say $z = hy$ for some $h \in G$, then we also have $z = hy = h(gx) = (hg)x$ such that $x \sim z$. Altogether $\sim$ is an equivalence relation on X. And for $x \in X$ the equivalence class of x is the orbit Gx, since

$$\begin{aligned} [x] &= \{\, y \in X \mid x \sim y \,\} \\ &= \{\, y \in X \mid \exists\, g \in G : y = gx \,\} \\ &= \{\, gx \mid g \in G \,\} \;=\; Gx \end{aligned}$$

(ii) We will first prove that the stabilizer $G^x = \{\, g \in G \mid gx = x \,\}$ is a subgroup of G. First of all $e \in G^x$ since $ex = x$. Also if $g, h \in G^x$ then $gx = x$ and $hx = x$ such that $(gh)x = g(hx) = gx = x$, and this means $gh \in G^x$ again. Finally $g \in G^x$ implies $x = ex = (g^{-1}g)x = g^{-1}(gx) = g^{-1}x$ such that $g^{-1} \in G^x$ again. Altogether G^x is a subgroup of G. It remains to prove the well-definedness and bijectivity of the map

$$Gx \to {}^{G}\big/_{G^x} \;:\; gx \mapsto gG^x$$

Let us first check the well-definedness: If $gx = hx$ then $(h^{-1}g)x = h^{-1}(gx) = h^{-1}(hx) = (h^{-1}h)x = ex = x$ such that $h^{-1}g \in G^x$. And this again is $gG^x = hG^x$ by definition of G/P. Now the surjectivity is clear: For $g \in G$ then $gx \in Gx$ is mapped to gG^x. And for the injectivity suppose we had some $g, h \in G$ with $gG^x = hG^x$. Undoing the above computation we then have $h^{-1}g \in G^x$ such that $gx = e(gx) = (hh^{-1})gx = h((h^{-1}g)x) = hx$ again.

(iii) By definition we have $gA \subseteq A$ for any $g \in G$. But this implies $A = eA = (gg^{-1})A = g(g^{-1}A)$. As $gA \subseteq A$ is also true for g^{-1} we continue $A = g(g^{-1}A) \subseteq gA \subseteq A$ such that $gA = A$.

(iv) Given $g \in G$ and $x \in X \setminus A$ we have to show $gx \in X \setminus A$. Thus suppose we had $gx \in A$, then we would conclude $x = ex = (g^{-1}g)x = g^{-1}(gx) \in g^{-1}A \subseteq A$, in contradiction to $x \in X \setminus A$.

(v) By (ii) we have $\#Gx = \#(G/G^x)$ and (as both, G and X are finite) by the theorem of Lagrange (1.7) this implies

$$\#Gx \;=\; [G : G^x] \;=\; \frac{\#G}{\#G^x}$$

Now the second orbit formula is a simple consequence: As $\sim$ is an equivalence relation the orbits Gx form a partition of X and hence

$$\#X \;=\; \sum_{Gx \in X/G} \#Gx \;=\; \#G \cdot \sum_{Gx \in X/G} \frac{1}{\#G^x}$$

(vi) The idea of this proof is the identity of the disjoint unions of the stabilizers $G^x = \{\, g \in G \mid gx = x \,\}$ and the fixed point sets $X^g = \{\, x \in X \mid gx = x \,\}$ below. Taking to the unions we find

$$\bigcup_{g \in G} \{\, g \,\} \times X^g \;=\; \{\, (g, x) \in G \times X \mid gx = x \,\} \;=\; \bigcup_{x \in X} G^x \times \{\, x \,\}$$

And as these unions are disjoint (by construction) we hence already have proved the second part of Burnsides formula

$$\sum_{g\in G} \#X^g \;=\; \sum_{x\in X} \#G^x$$

For the first part we use the partition of X into orbits Gx again, that is $X = \bigcup Gx$ where the union runs over all orbits $Gx \in X/G$. This can be used to split the sum over all $x \in X$ into two separate sums the first over $Gx \in X/G$ the second over $y \in Gx$

$$\sum_{x\in X} \#G^x \;=\; \sum_{Gx\in X/G} \sum_{y\in Gx} \#G^x \;=\; \sum_{Gx\in X/G} \#Gx \cdot \#G^x$$

But by the orbit fomula in (iv) we have $\#Gx \cdot \#G^x = \#G$ identically, such that this sum is reduced once again, leaving only

$$\sum_{x\in X} \#G^x \;=\; \sum_{Gx\in X/G} \#G \;=\; \#G \cdot \#{}^{X}\big/_{G}$$

□

15.2 Proofs of Chapter 1

In order to be able to provide the proofs of the first introductory chapter to algebra, we have to make some preparations: Division with remainder in the integers and we promised to present a way to deal with bracketing formally. We chose to keep the latter out of the main text, as it is rather formal and little suited for a beginners in algebra. As we want to stay rigorous, we chose to present it nevertheless, so this only leaves a place in the back yard - here. We also pulled up front some elementary proofs, that should be done, as soon as possible.

Division with Remainder:
Consider any $d \in \mathbb{N}$ with $d \geq 1$ which we call the *divisor*. Then for any $x \in \mathbb{Z}$ there are uniquely determined $q, r \in \mathbb{Z}$ such that

(1) $x = qd + r$

(2) $r \in 0 \dots (d-1)$

This result will be largely generalized in section 2.7 and proved in greater generality, but as we use this fact for $\mathbb{Z}$ we have to give a proof beforehand. The numbers q and r in the statement above can even be given explicitly

$$\begin{aligned} q &= x \text{ div } d &:=& \quad \max\{\, k \in \mathbb{Z} \mid kd \leq x \,\} \\ d &= x \text{ mod } d &:=& \quad x - (x \text{ div } d) \cdot d \end{aligned}$$

Prob *Existence:* as $x \leq |x| \leq |x| \cdot d$ then set $\{\, k \in \mathbb{Z} \mid kd \leq x \,\}$ is bounded from above by $|x|$. Hence the maximum $q := \max\{\, k \in \mathbb{Z} \mid kd \leq x \,\}$ is well defined. Also take $r := x - qd \in \mathbb{Z}$. Then (1) $x = qd + r$ is clear from the definition of r and as $qd \leq x$ we also have $r \geq 0$. Now suppose $r \geq d$ then we would have $0 \leq r - d = x - qd - d = x - (q+1)d$ such that $(q+1)d \leq x$. But as q has been maximal, this is absurd, which only leaves $r < d$, such that (2) is established, as well.
Uniqueness: suppose $x = qd + r$ and $x = ud + v$ for some q, r, u and $v \in \mathbb{Z}$ with r and $v \in 0 \dots (d-1)$. Then $0 = x - x = qd + r - (ud + v) = (q-u)d + r - v$. That is d divides $(q-u)d = v - r$. But as $0 \leq v$, $r < d$ we have $|v - r| < d$ and hence $v - r$ can only be divided by d, if $v - r = 0$. That is $r = v$ and therefore $qd + r = ud + v$ implies $qd = ud$ which also yields $q = u$. □

Formal Bracketing $(\diamondsuit)$
If we multiply (or sum up) several elements $x_1, \dots, x_n \in G$ of a groupoid $(G, \circ)$ we've got $(n-1)$ possibilities, with which two elements we start - even if we keep their ordering. And we have to keep choosing until we finally got one element of G. In this light it is quite clear, what we mean by saying "any way of applying parentheses to the product of the x_i results in the same element". It just says, that the result actually doesn't depend on our choices. However - as we do math - we wish to give a formal way of putting this. To do this first define a couple mappings for $2 \leq n \in \mathbb{N}$ and $k \in 2 \dots (n-2)$

$$\begin{aligned} b_{(n,1)} &: G^n \to G^{n-1} : (x_1, \dots, x_n) \mapsto (x_1 x_2, x_3, \dots, x_n) \\ b_{(n,k)} &: G^n \to G^{n-1} : (x_1, \dots, x_n) \mapsto (x_1, \dots, x_k x_{k+1}, \dots, x_n) \\ b_{(n,n-1)} &: G^n \to G^{n-1} : (x_1, \dots, x_n) \mapsto (x_1, \dots, n_{n-2}, x_{n-1} x_n) \end{aligned}$$

Now we can determine the sequel of choosing the parentheses simply by selecting an $(n-1)$-tupel k in the following set

$$D_n \;:=\; \{\, k=(k_1,\ldots,k_{n-1}) \mid k_i \in 1\ldots(n-i) \text{ for } i \in 1\ldots(n-1)\,\}$$

For fixed $k \in D_n$ the *bracketing* (by k) now simply is the following mapping

$$B_k \;:=\; b_{(2,k_{n-1})} \circ \cdots \circ b_{(n,k_1)} \;:\; G^n \to G$$

Proof of (1.2) (associativity): $(\diamondsuit)$
We now wish to prove the fact that in a groupoid $(G,\circ)$ the product of the elements $x_1,\ldots,x_n$ is independent of the order in which we applied parentheses to it. Formally this can now be put as: for any $k \in D_n$ we get

$$B_k(x_1,\ldots,x_n) \;=\; x_1x_2\ldots x_n$$

We will prove this statement by induction on the number n of elements multiplied. In the cases $n=1$ and $n=2$ there only is one possibility how to apply parentheses and hence the statement is trivial. The case $n=3$ there are two possibilities, which are equal due to the associativity law (A) of $(G,\circ)$. Thus we assume $n>3$ and regard two ways of applying parentheses $k,l \in D_n$, writing them in terms of the last multiplication used

$$\begin{aligned} a \;:=\; B_k(x_1,\ldots,x_n) &= B_p(x_1,\ldots,x_i)B_p(x_{i+1},\ldots,x_n) \\ b \;:=\; B_l(x_1,\ldots,x_n) &= B_q(x_1,\ldots,x_j)B_q(x_{j+1},\ldots,x_n) \end{aligned}$$

where $i := k_1$, $j := l_1$ and $p := (k_2,\ldots,k_{n-1})$, $q := (l_2,\ldots,l_{n-1})$. We may assume $i \le j$ and if $i=j$ we are already done because of the induction hypothesis. Thus we have $i<j$ and by the induction hypothesis the parentheses may be rearranged to

$$\begin{aligned} a &= \Big((x_1\ldots x_i)\Big((x_{i+1}\ldots x_j)(x_{j+1}\ldots x_n)\Big)\Big) \\ b &= \Big(\Big((x_1\ldots x_i)(x_{i+1}\ldots x_j)\Big)(x_{j+1}\ldots x_n)\Big) \end{aligned}$$

Now the associativity law again implies $a=b$ and as k and l were arbitrary this implies $a = x_1x_2\ldots x_n$ for any bracketing k chosen. □

Proof of (1.5):

- Let $(G,\circ)$ be any group, then $ee=e=ee$ and hence $e=e^{-1}$ by definition of the inverse element. Likewise if $y=x^{-1}$ then $xy=e=yx$ and hence $x=y^{-1}$. Then we prove $(xy)^{-1}=y^{-1}x^{-1}$ by

$$\begin{aligned} (xy)(y^{-1}x^{-1}) &= x\Big(y(y^{-1}x^{-1})\Big) \;=\; x\Big((yy^{-1})x^{-1}\Big) \\ &= x\Big(ex^{-1}\Big) \;=\; xx^{-1} \;=\; e \\ (y^{-1}x^{-1})(xy) &= y^{-1}\Big(x^{-1}(xy)\Big) \;=\; y^{-1}\Big((x^{-1}x)y\Big) \\ &= y^{-1}\Big(ey\Big) \;=\; y^{-1}y \;=\; e \end{aligned}$$

- Next we will prove $(x^k)^{-1} = (x^{-1})^k$ by induction on $k \geq 0$. If $k = 0$ then the claim is satisfied, as $e^{-1} = e$. Now we conduct the induction step, using what we have just proved:

$$\left(x^{k+1}\right)^{-1} \;=\; \left(x^k x\right)^{-1} \;=\; x^{-1}\left(x^k\right)^{-1} \;=\; x^{-1}\left(x^{-1}\right)^k \;=\; \left(x^{-1}\right)^{k+1}$$

- Now assume that $xy = yx$ do commute. Then it is easy to see that $x^{-1}y^{-1} = y^{-1}x^{-1} = (xy)^{-1}$ do commute as well, just compute

$$y^{-1}x^{-1} \;=\; (xy)^{-1} \;=\; (yx)^{-1} \;=\; x^{-1}y^{-1}$$

 And by induction on $k \geq 0$ it also is clear, that $x^k y = yx^k$. Now we will prove $(xy)^k = x^k y^k$ by induction on k. In the case $k = 0$ everything is clear $(xy)^0 = e = ee = x^0 y^0$. Now compute

$$\begin{aligned}\left(xy\right)^{k+1} &= \left(xy\right)^k\left(xy\right) \;=\; \left(x^k y^k\right)\left(yx\right)\\ &= x^k\left(y^k(yx)\right) \;=\; x^k\left(y^{k+1}x\right)\\ &= x^k\left(xy^{k+1}\right) \;=\; x^{k+1}y^{k+1}\end{aligned}$$

 And for negative k we regard $-k$ where $k \geq 0$, then we easily compute

$$\begin{aligned}\left(xy\right)^{-k} &= \left((xy)^{-1}\right)^k \;=\; \left(x^{-1}y^{-1}\right)^k\\ &= \left(x^{-1}\right)^k\left(y^{-1}\right)^k \;=\; x^{-k}y^{-k}\end{aligned}$$

- Note: in the last step of the above we have used $(x^{-1})^k = x^{-k}$. But we still have to prove this equality: as for any $x \in G$ we find that $xx^{-1} = e = x^{-1}x$ do commute we also obtain $x^{-k} = (x^k)^{-1} = (x^{-1})^k$ for any $k \geq 0$, just compute

$$x^{-k}x^k \;=\; \left(x^{-1}\right)^k x^k \;=\; \left(x^{-1}x\right)^k \;=\; e^k \;=\; e$$

$$x^k x^{-k} \;=\; x^k\left(x^{-1}\right)^k \;=\; \left(xx^{-1}\right)^k \;=\; e^k \;=\; e$$

- This also allows us to prove $(x^k)^l = x^{kl}$ for any $k, l \in \mathbb{Z}$. We will distinguish four cases - to do this assume $k, l \geq 0$ then

$$\left(x^k\right)^l \;=\; x^k x^k \ldots x^k \;\; (l - \text{times}) \;=\; x^{kl}$$

$$\left(x^{-k}\right)^l \;=\; \left((x^{-1})^k\right)^l \;=\; \left(x^{-1}\right)^{kl} \;=\; x^{-(kl)} \;=\; x^{(-k)l}$$

$$\left(x^k\right)^{-l} \;=\; \left((x^k)^{-1}\right)^l \;=\; \left((x^{-1})^k\right)^l \;=\; x^{-(kl)} \;=\; x^{k(-l)}$$

$$\left(x^{-k}\right)^{-l} = \left(((x^{-1})^k)^{-1}\right)^l = \left(((x^k)^{-1})^{-1}\right)^l \;=\; x^{kl} \;=\; x^{(-k)(-l)}$$

- It remains to prove $x^k x^l = x^{k+l}$ for any $k, l \in \mathbb{Z}$. As above we will distinguish four cases, that is

we regard $k, l \geq 0$. In this case $x^k x^l = x^{k+l}$ is clear by definition. Further we can compute

$$x^{-k}x^{-l} \;=\; \left(x^{-1}\right)^k \left(x^{-1}\right)^l \;=\; \left(x^{-1}\right)^{k+l} \;=\; x^{-(k+l)} \;=\; x^{(-k)+(-l)}$$

For the remaining two cases we first show $x^{-1}x^l = x^{l-1}$. In case $l \geq 0$ this is immediately clear. And in case $l \leq 0$ we regard $-l$ with $l \geq 0$

$$x^{-1}x^{-l} \;=\; x^{-1}\left(x^{-1}\right)^l \;=\; \left(x^{-1}\right)^{l+1} \;=\; x^{-(l+1)} \;=\; x^{(-l)-1}$$

We are now able to prove $x^{-k}x^l = x^{(-k)+l}$ by induction on k. The case $k = 0$ is clear, for the induction step we compute

$$x^{-(k+1)}x^l = (x^{-1})^k x^{-1}x^l = (x^{-1})^k x^{-1}x^l = x^{-k}x^{l-1} = x^{-(k+1)+l}$$

The fourth case finally is $x^k x^{-l} = x^{k+(-l)}$, but as x^k and x^{-l} commute (use inductions on k and l) this readily follows the above.

□

Proof of (1.7):
The first statement that needs to be verified is that a subgroup $P \leq_g G$ truly invokes an equivalence relation $x \sim y \iff y^{-1}x \in P$. This relation clearly is reflexive: $x \sim x$ due to $x^{-1}x = e \in P$. And it also is transitive because if $x \sim y$ and $y \sim z$ then $y^{-1}x \in P$ and $z^{-1}y \in P$. Thereby $z^{-1}x = z^{-1}(yy^{-1})x = (z^{-1}y)(y^{-1}x) \in P$ too, which again means $x \sim z$. Finally it is symmetric as well: if $x \sim y$ then $y^{-1}x \in P$ and hence $x^{-1}y = (y^{-1}x) \in P$ too, which is $y \sim x$. Next we wish to prove that truly $[x] = xP$

$$\begin{aligned} [x] \;&=\; \{\, y \in G \mid y \sim x \,\} \;=\; \left\{\, y \in G \mid x^{-1}y = p \in P \,\right\} \\ &=\; \{\, y \in G \mid \exists\, p \in P : y = xp \,\} \;=\; \{\, xp \mid p \in P \,\} \;=\; xP \end{aligned}$$

So it only remains to prove the theorem of Lagrange. To do this we fix a system $\mathbb{P}$ of representatives of G/P. That is we fix a subset $\mathbb{P} \subseteq G$ such that $\mathbb{P} \longleftrightarrow G/P : q \mapsto qP$ (which is possible due to the axiom of choice). Then we obtain a bijection by letting

$$G \longleftrightarrow \left(G \Big/ P\right) \times P \;:\; x \mapsto \left(xP,\; q^{-1}x \text{ where } xP = qP\right)$$

This map is well defined: as $xP \in G/P$ there is a uniquely determined $q \in \mathbb{P}$ such that $qP = xP$. And for this we get $q \sim x$ which means $q^{-1}x \in P$. And it is injective: if $xP = yP = qP$ then $q^{-1}x = q^{-1}y$ yields $x = y$ (by multiplication with q). Finally it also is surjective: given (qP, p) we let $x := qp \in qP$ and thereby obtain $q \sim x$ and hence $(xP, q^{-1}x) = (qP, p)$. □

Proof of (1.8):
We first have to prove, that $\langle X \rangle_o$ is a well-defined submonoid of G. As $X \subseteq G$ and G is a submonoid, the intersection runs over a non-empty set and hence is well-defined. Also, as $e \in X_e$, we clearly have $e \in \langle X \rangle_o$. And if x and $y \in \langle X \rangle_o$ then for any $P \leq_o G$ with $X \subseteq P$ we have $x, y \in P$. But as P is a submonoid this implies $xy \in P$ again and as this is true for any P we also get $xy \in \langle X \rangle_o$ again.
Likewise if G is a group, then (by the same arguments as above) $\langle X \rangle_g$ is a submonoid of G. It remains to

prove that it even is a subgroup: But as P is a subgroup this implies $x^{-1} \in P$ again and as this is true for any P we also get $x^{-1} \in \langle X \rangle_o$ again.
Next we will prove the explict representation of $\langle X \rangle_o$, to to this let us denote the set of finite products of elements of X_e by

$$Q \;:=\; \{\, x_1 x_2 \dots x_n \mid n \in \mathbb{N},\, x_1, \dots, x_n \in X_e \,\}$$

As $e \in X_e$ it is clear that $e \in Q$. And if $x = x_1 \dots x_m$ and $y = y_1 \dots y_n \in Q$ then by construction we also have $xy \in Q$. That is: Q is a submonoid of G and as $X \subseteq Q$ is clear we have $\langle X \rangle_o \subseteq Q$. Conversely, as $\langle X \rangle_o$ is a monoid with $X \subseteq \langle X \rangle_o$ we have e and $x \in \langle X \rangle_o$ for any $x \in X$. That is $X_e \subseteq \langle X \rangle_o$. Therefore, if $x_1, \dots, x_n \in X_e$ then $x_1 \dots x_n \in \langle X \rangle_o$ again and this also is $Q \subseteq \langle X \rangle_o$. Together we have $Q = \langle X \rangle_o$.
We finally have to prove the explicit representation of $\langle X \rangle_g$, to do this let us abbreviate the set of finite products of elements of $X_\pm$ by

$$Q \;:=\; \{\, x_1 x_2 \dots x_n \mid n \in \mathbb{N},\, x_1, \dots, x_n \in X_\pm \,\}$$

If $x \in X$ we also have $x^{-1} \in X_\pm$ and as $(x^{-1})^{-1} = x$ we find that $x^{-1} \in X_\pm$ for any $x \in X_\pm$. That is $X_\pm$ is closed under the inversion of elements. Also $e \in X_\pm$ is trivial. And if $x = x_1 \dots x_m$ and $y = y_1 \dots y_n \in Q$ then by construction we also have $xy \in Q$. But also $x^{-1} = x_m^{-1} \dots x_1^{-1} \in Q$, as with $x_i \in X_\pm$ we also have $x_i^{-1} \in X_\pm$. Hence Q is a subgroup of G and as $X \subseteq Q$ is clear we have $\langle X \rangle_g \subseteq Q$. Conversely, as $\langle X \rangle_g$ is a group with $X \subseteq \langle X \rangle_g$ we have e, x and $x^{-1} \in \langle X \rangle_g$ for any $x \in X$. That is $X_\pm \subseteq \langle X \rangle_g$. Therefore, if $x_1, \dots, x_n \in X_\pm$ then $x_1 \dots x_n \in \langle X \rangle_g$ again and this also is $Q \subseteq \langle X \rangle_g$. Together we have $Q = \langle X \rangle_g$. □

Proof of (1.9):
It is clear that $Q := \{\, x^k \mid k \in \mathbb{Z} \,\}$ is a subgroup of G, as for any $i, j \in \mathbb{Z}$ we have $x^i x^j = x^{i+j} \in Q$ and $(x^i)^{-1} = x^{-i} \in Q$. Also, as $x \in Q$ we get $\langle x \rangle_g \subseteq Q$. But as $x \in \langle x \rangle_g$ and $\langle x \rangle_g$ is a group we clearly have $x^k \in \langle x \rangle_g$ for any $k \in \mathbb{Z}$ and hence $Q \subseteq \langle x \rangle_g$ as well. Altogether $\langle x \rangle_g = Q$.
Now suppose $n := \#G \in \mathbb{N}$ is finite, then $Q \subseteq G$ is finite, too, say $k := \#Q$. If now $i, j \in \mathbb{N}$ with $i < j$ then (by multiplication with x^{-i} from the left) we clearly have

$$x^i \;=\; x^j \quad\Longleftrightarrow\quad x^{j-i} \;=\; e$$

Thus if we had $x^p \neq e$ for any $p \in \mathbb{N}$ then $x^i \neq x^j$ for any $i < j$ and hence $\langle x \rangle_g$ had infinitely many elements. As this is untrue, there has to be some $p \in \mathbb{N}$ with $1 \leq p$ such that $x^p = e$. Let $m \in \mathbb{N}$ be the minimal such number

$$m \;:=\; \min\{\, 1 \leq p \in \mathbb{N} \mid x^p = e \,\}$$

As $x^m = e$ is the first occurance of e we have $x^i \neq e$ for any $1 \leq i < m$. And this implies $x^i \neq x^j$ for any $i, j \in \mathbb{N}$, with $i \neq j$ and $i, j < m$. Hence we have found m distinct elements in $\langle x \rangle_g$, namely

$$\left\{\, x^i \mid i \in 0 \dots (m-1) \,\right\} \quad\subseteq\quad \langle x \rangle_g$$

Conversely consider any $x^q \in \langle x \rangle_g$ and write $q = pm + i$ by division of q by m with remainder $i \in 0 \dots (m-1)$. Then $x^q = x^{pm+i} = (x^m)^p x^i = e^p x^i = x^i$. That is $\langle x \rangle_g$ only consists of elements of the form x^i for some $0 \leq i < m$ and hence the above sets even are equal. In particular we have $m = k$. And

as $\langle x \rangle_g$ is a subgroup of G the theorem of Lagrange (1.7) truly implies $k \mid n$.
Let us finally prove $x^n = e$: To see this let $k := \mathrm{ord}(x)$, in particular $x^k = e$. As we have just seen $k \mid n$ there is some $q \in \mathbb{Z}$ such that $n = qk$. And thereby $x^n = x^{qk} = (x^k)^q = e^q = e$. □

Proof of (1.10):
If σ and $\tau : X \to X$ then the composition $\sigma\tau : x \mapsto \sigma(\tau(x))$ is another map of the form $\sigma\tau : X \to X$. And if both σ and τ are bijective, so is $\sigma\tau$ with inverse $(\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1}$. Hence S_X is closed under the compositon $\circ$. And the associativity of the composition is well-known. Also $\mathbb{1}_X : x \mapsto x$ is bijective and hence $\mathbb{1}_X \in S_X$. Hence $(S_X, \circ)$ is a monoid. And as σ^{-1} is the inverse element of σ and bijective again we have $\sigma^{-1} \in S_X$ again, such that S_X is a group. □

Proof of (1.12):

(i) By induction on the number of elements $n := \#X$: In case $n = 1$ we have $X = \{ x \}$ for some single element $x \in X$. Hence the one any only map on X is given to be $\sigma(x) = x$. In particular $\#S_X = 1 = 1! = (\#X)!$. Now for the induction step we consider a set with $n+1$ elements $X = \{ x_1, \ldots, x_n, x_{n+1} \}$. Then we can decompose S_X into the following disjoint union

$$S_X \;=\; \bigcup_{i=1}^{n+1} F(i) \quad \text{where} \quad F(i) \;:=\; \{ \sigma \in S_X \mid \sigma(x_{n+1}) = x_i \}$$

Clearly, if $\sigma(x_{n+1}) = x_i$, then σ induces a bijection between the sets $X(i) := X \setminus \{ x_i \}$ and $X(n+1)$. As $X(i)$ always contains n elements we can choose a bijection $\alpha_i : X(i) \longleftrightarrow X(n+1)$. And this now gives rise to a bijection between

$$F(i) \longleftrightarrow S_{X(n+1)} \;:\; \sigma \mapsto \alpha_i \sigma\big|_{X(n+1)}$$

In particular for any $i \in 1 \ldots n+1$ the set $F(i)$ contains as many elements, as $S_{X(n+1)}$. And by induction hypothesis, as $\#X(n+1) = n$ this is $n!$. So altogether

$$\#S_X \;=\; \sum_{i=1}^{n+1} \#F(i) \;=\; (n+1)\, n! \;=\; (n+1)!$$

(ii) Let us define an equivalence relation on S_{n+1} by letting $\varrho \sim \sigma$ if and only if $\varrho(n+1) = \sigma(n+1)$. Then it is clear that the equivalence classes of this relation are precisely the sets

$$E_k \;:=\; \{ \sigma \in S_{n+1} \mid \sigma(n+1) = k \}$$

where k runs from 1 to $n+1$. E.g. the transposition τ_k belongs to E_k (that is $[\tau_k] = E_k$) since $\tau_k(n+1) = k$. In particular the sets E_k form a pairwise disjoint [i.e. for any $i \neq j \in 1 \ldots n+1$ we have $E_i \cap E_j = \emptyset$] union of S_{n+1}. So it only remains to prove the equality of the sets

$$E_k \;=\; \tau_k S'_n \;=\; \{ \tau_k \pi \mid \pi \in S'_n \}$$

For the inclusion " $\supseteq$ " we are given some $\pi \in S'_n$ and have to regard $\sigma := \tau_k \pi$. But clearly $\sigma(n+1) = \tau_k \pi(n+1) = \tau_k(n+1) = k$ such that $\sigma \in E_k$. Conversely, if $\sigma(n+1) = k$ then we define $\pi := \tau_k \sigma$ and find $\pi(n+1) = \tau_k \sigma(n+1) = \tau_k(k) = n+1$. Thereby $\pi \in S'_n$ and

$\tau_k\pi = \tau_k^2\sigma = \sigma$ such that we find $\sigma \in \tau_k S_n'$ as well.

(iii) First of all we see that for any g, h and $x \in G$ the associativity of G gives birth to the following equality: $L_{gh}(x) = (gh)x = g(hx) = L_g(hx) = L_g(L_h(x)) = L_g L_h(x)$. And as $x \in G$ has been arbitrary this is $L_{gh} = L_g L_h$. Also it is clear that $L_e(x) = ex = x = \mathbb{1}_G(x)$ such that $L_e = \mathbb{1}_G$. In particular $L_{g^{-1}}$ is the inverse map of L_g since

$$L_{g^{-1}}L_g \;=\; L_{g^{-1}g} \;= L_e \;=\; \mathbb{1}_G$$

$$L_g L_{g^{-1}} \;=\; L_{gg^{-1}} \;= L_e \;=\; \mathbb{1}_G$$

In particular $L_g : G \to G$ not only is a map, but even a bijective one. Hence $L_g \in S_G$ and this makes L well-defined. It remains to show the injectivity of L but this is easy: if $L_g = L_h$ then $g = ge = L_g(e) = L_h(e) = he = h$.

□

Proof of (1.14):

(i) As $n = \#X$ is finite S_X is a finite group with $n!$ elements. And as $S := \{\, \sigma^k \mid k \in \mathbb{Z} \,\}$ is a subgroup of the finite group S_X [this has been shown in (1.12.(i))], we know from (1.9), that there is some $k \in \mathbb{N}$ with $\sigma^k = \mathbb{1}$, say $k = \mathrm{ord}(\sigma)$. In particular $\sigma^k(x) = x$ such that the cycle $\mathrm{cyc}(\sigma, x)$ if finite, with $\ell(\sigma, x) \leq k = \mathrm{ord}(\sigma)$.

(ii) If $x \in \mathrm{fix}(\sigma)$, then $\sigma(x) = x$, by definition. In particular we have $\sigma(x) \in \mathrm{fix}(\sigma)$ for any $x \in \mathrm{fix}(\sigma)$ and thereby $\sigma(\mathrm{fix}(\sigma)) \subseteq \mathrm{fix}(\sigma)$. Conversely regard some $x \in \mathrm{fix}(\sigma)$ and let $u := \sigma^{-1}(x) \in X$. Then $\sigma(u) = x \in \mathrm{fix}(\sigma)$. That is $\sigma(\sigma(u)) = \sigma(u)$. As σ is injective, we conclude $\sigma(u) = u$ and thereby $u \in \mathrm{fix}(\sigma)$ again. That is $x = \sigma(u) \in \sigma(\mathrm{fix}(\sigma))$ and this is the converse inclusion $\mathrm{fix}(\sigma) \subseteq \sigma(\mathrm{fix}(\sigma))$. Altogether

$$\sigma\big(\mathrm{fix}(\sigma)\big) \;\subseteq\; \mathrm{fix}(\sigma)$$

Now for the domain of σ: Suppose we had $y := \sigma(x) \in \mathrm{fix}(\sigma)$, then we had $\sigma(y) = y = \sigma(x)$. But as σ is injective this would imply $x = y \in \mathrm{fix}(\sigma)$ which is absurd, since we started with $x \in \mathrm{dom}(\sigma)$. This is the inclusion $\sigma(\mathrm{dom}(\sigma)) \subseteq \mathrm{dom}(\sigma)$. Conversely regard some $x \in \mathrm{dom}(\sigma)$ and let $u := \sigma^{-1}(x) \in X$. Suppose we had $u \in \mathrm{fix}(\sigma)$, then $x = \sigma(u) = u$ such that $\sigma(x) = \sigma(u) = x$ in contradiction to $x \in \mathrm{dom}(\sigma)$. Thus we have $u \in \mathrm{dom}(\sigma)$ again and thereby $x = \sigma(x) \in \sigma(\mathrm{dom}(\sigma))$, which is the converse inclusion. Altogether we also found

$$\sigma\big(\mathrm{dom}(\sigma)\big) \;\subseteq\; \mathrm{dom}(\sigma)$$

If now $x \in \mathrm{dom}(\sigma)$ then we will use induction on k to prove that any $\sigma^k(x)$ lies within $\mathrm{dom}(\sigma)$: The case $k = 0$ is true by assumption $\sigma^0(x) = x \in \mathrm{dom}(\sigma)$. Now $\sigma^{k+1}(i) = \sigma(\sigma^k(x))$ and by induction hypothesis we know $\sigma^k(x) \in \mathrm{dom}(\sigma)$. Hence $\sigma^{k+1}(x) \in \sigma(\mathrm{dom}(\sigma)) = \mathrm{dom}(\sigma)$ again.

(iii) If $\varrho = \sigma$ then $\mathrm{dom}(\varrho) = \mathrm{dom}(\sigma)$ and $\varrho(x) = \sigma(x)$ for any $x \in D$ are trivial, as we even have $\varrho(x) = \sigma(x)$ for any $x \in X$. Conversely let $D = \mathrm{dom}(\varrho) = \mathrm{dom}(\sigma)$. If $x \in D$ then $\varrho(x) = \sigma(x)$ by assumption. But if $x \notin D$ then we have $x \in \mathrm{fix}(\varrho)$ and $x \in \mathrm{fix}(\sigma)$ such that $\varrho(x) = x = \sigma(x)$. Hence we have $\varrho(x) = \sigma(x)$ for any $x \in X$ and this is $\varrho = \sigma$, as claimed.

(iv) If $x \in \mathrm{dom}(\varrho)$ then by assumption we have $x \notin \mathrm{dom}(\sigma)$ such that $x \in \mathrm{fix}(\sigma)$. In particular we get

$$\varrho\sigma(x) \;=\; \varrho(x)$$

And as we know $\varrho(x) \in \mathrm{dom}(\varrho)$ again, because of (ii), we likewise have $\varrho(x) \in \mathrm{fix}(\sigma)$ such that we also find

$$\sigma\varrho(x) \;=\; \varrho(x)$$

That is $\varrho\sigma(x) = \varrho(x) = \sigma\varrho(x)$ for any $x \in \mathrm{dom}(\varrho)$. In complete analogy (by interchanging the roles of ϱ and σ) we find (for any $x \in \mathrm{dom}(\sigma)$)

$$\sigma\varrho(x) \;=\; \sigma(x) \;=\; \varrho\sigma(x)$$

And if finally $x \in X \setminus (\mathrm{dom}(\varrho) \cup \mathrm{dom}(\sigma)) = \mathrm{fix}(\varrho) \cap \mathrm{fix}(\sigma)$ then it is clear that $\varrho\sigma(x) = \varrho(x) = x$ and also $\sigma\varrho(x) = \sigma(x) = x$. In any case we have seen (for any $x \in X$) that $\varrho\sigma(x) = \sigma\varrho(x)$, which is the commutativity $\varrho\sigma = \sigma\varrho$.

□

Proof of (1.16):

- As long as the order of the i_k is maintained, we still have $i_k \mapsto i_{k+1}$ (and $i_\ell \mapsto i_1$) no matter with wich element i_k we begin. Hence

$$(i_1\, i_2\, \ldots\, i_\ell) \;=\; (i_2\, i_3\, \ldots\, i_\ell\, i_1) \;=\; \ldots \;=\; (i_\ell\, i_1\, i_2\, \ldots\, i_{\ell-1})$$

- Let us denote $\zeta := (i_1\; i_\ell)(i_1\; i_{\ell-1}) \ldots (i_1\; i_2)$, then given any $a = i_q$ let us regard ζ from the right: i_q is unaffected by any $(i_1\; i_p)$ with $p < q$. Hence i_q it first hits $(i_1\; i_q)$ which maps $i_q \to i_1$. Now i_1 immediatley strikes $(i_1\; i_{q+1})$ again mapping $i_1 \mapsto i_{q+1}$. And i_{q+1} passes through unhampered, as it only meets $(i_1 i_r)$ whith $r > q+1$ from now on. Altogether we have $\zeta : i_q \mapsto i_1 \mapsto i_{q+1}$. A special case is $a = i_\ell$ as this only strikes $(i_1 i_\ell)$ at the very end, such that $\zeta : i_\ell \mapsto i_1$. Therefore $\zeta = (i_1\; i_2\; \ldots\; i_\ell)$.

- By induction on $d := j - i \in \mathbb{N}$. The case $d = 1$ is trivial, as $(i\; j) = (i\; i+1)$ in this case. For $d \geq 2$ we have to regard $(i\; j) = (i\; i+d)$. To do this we first prove that $(i\; i+d) = (i\, i+1)(i+1\; i+d)(i\, i+1)$ by explicitly computing (from right to left):

$$\begin{array}{ccccccc}
 & (i\, i+1) & & (i+1\, i+d) & & (i\, i+1) & \\
i+d & \hookleftarrow & i+d & \hookleftarrow & i+1 & \hookleftarrow & i \\
i+1 & \hookleftarrow & i & \hookleftarrow & i & \hookleftarrow & i+1 \\
i & \hookleftarrow & i+1 & \hookleftarrow & i+d & \hookleftarrow & i+d
\end{array}$$

 As the domain of $\zeta = (i\; i+1)(i+1\; i+d)(i\; i+1)$ is $\mathrm{dom}(\zeta) = \{\, i, i+1, i+d \,\}$ it is clear, that $\zeta(a) = a$ for any $a \notin \{\, i, i+1, i+d \,\}$. And as $\zeta(i) = i+d$, $\zeta(i+1) = i+1$ and $\zeta(i+d) = i$ we have truly shown that $\zeta = (i\; i+d)$. But by induction hypothesis $(i+1\; i+d)$ is of distance $d-1$ and can hence be written as

$$(i+1\;\; i+d) \;=\; (i+1\;\; i+2) \ldots (i+d-1\;\; i+d) \ldots (i+1\;\; i+d)$$

Inserting this into $(i\ i+d) = (i\ i+1)(i+1\ i+d)(i\ i+1)$ we have also proved the case $d \geq 2$ and hence for any transposition, as d may be arbitrarily large.

- Let us denote the cycle $\xi := (\sigma(i_1)\ \sigma(i_2)\ \ldots\ \sigma(i_\ell))$. Then is is clear that $\mathrm{dom}(\xi) = \{\sigma(i_1), \sigma(i_2), \ldots, \sigma(i_\ell)\}$ and for any $k \in 1 \ldots \ell - 1$ we have $\xi(\sigma(i_k)) = \sigma(i_{k+1})$, also $\xi(\sigma(i_\ell)) = \sigma(i_1)$. But on the other hand it is easy to compute $\sigma\zeta\sigma^{-1}(\sigma(i_k)) = \sigma\zeta(i_k) = \sigma(i_{k+1})$ and likewise $\sigma\zeta\sigma^{-1}(\sigma(i_\ell)) = \sigma\zeta(i_\ell) = \sigma(i_1)$. Hence we have seen $\sigma\zeta\sigma^{-1}(a) = \xi(a)$ for any $a = \sigma(i_k)$ (where $k \in 1 \ldots \ell$). If now $a \in 1 \ldots n$ is none of the $\sigma(i_k)$ (that is $a \notin \mathrm{dom}(\xi)$) then $\sigma^{-1}(a) \notin \{i_1, i_2, \ldots, i_\ell\} = \mathrm{dom}(\zeta)$. Therefore we have $\sigma\zeta\sigma^{-1}(a) = \sigma(\sigma^{-1}(a)) = a = \xi(a)$ again. That is $\sigma\zeta\sigma^{-1}$ and ξ share the same domain and agree on it, such that by (1.14.(iii)) they are equal.

□

Proof of (1.17):

- (a) $\Longrightarrow$ (b): by assumption we have $\sigma = (i_1\ i_2\ \ldots\ i_\ell)$ for some pairwise distinct $i_k \in 1 \ldots n$. Therefore it is clear that

$$\mathrm{dom}(\sigma) \ = \ \{i_1, i_2, \ldots, i_\ell\}$$

 Let us abbreviate $i := i_1$, then by induction on k it is clear that $i_k = \sigma^{k-1}(i)$, because $\sigma^k(i) = \sigma(\sigma^{k-1}(i)) = \sigma(i_k) = i_{k+1}$. If we are now given any $a, b \in \mathrm{dom}(\sigma)$, then there are r and $s \in 1 \ldots \ell$ such that $a = i_r = \sigma^{r-1}(i)$ and $b = i_s = \sigma^{s-1}(i)$. If $s \geq r$ then we can readily take $k := s - r \in \mathbb{N}$ to see

$$\sigma^k(a) \ = \ \sigma^{s-r}\sigma^{r-1}(i) \ = \ \sigma^{s-1}(i) \ = \ b$$

 And if $s < r$ then we take $k := \ell + s - r \in \mathbb{N}$ (which is positive, since $r \leq \ell$). Note that $\sigma^\ell(i) = \sigma\sigma^{\ell-1}(i) = \sigma(i_\ell) = i_1$ such that we can likewise compute

$$\sigma^k(a) \ = \ \sigma^{\ell+s-r}\sigma^{r-1}(i) \ = \ \sigma^{s-1}\sigma^\ell(i) \ = \ = \ \sigma^{s-1}(i) \ = \ b$$

 Thus in any case we have seen that $b = \sigma^k(i)(a)$ which had to be shown.

- (b) $\Longrightarrow$ (c): choose any $i \in \mathrm{dom}(\sigma)$ then by assumption we have $b = \sigma^k(i)$ for any $b \in \mathrm{dom}(\sigma)$ for some sufficient $k \in \mathbb{N}$. That is

$$\mathrm{dom}(\sigma) \ \subseteq \ \left\{ \sigma^k(i) \mid k \in \mathbb{N} \right\}$$

 But the converse inclusion is a generat truth, for any permutation, as we have shown in (1.18.(ii)). And hence the above inclusion even is an equality of sets. Now (c) $\Longrightarrow$ (d) is trivial - note that $\mathrm{dom}(\sigma) \neq \emptyset$ is nonempty, as we assumed $\sigma \neq \mathbb{1}$.

- (d) $\Longrightarrow$ (e): all we have to do is prove, that the higher powers k of $\sigma^k(i)$ are already contained in $\{\sigma^r(i) \mid r \in 0 \ldots \ell - 1\}$. So consider any $k \geq \ell$, then we use division with remainder to write k as $k = m\ell + r$ for some $m \in \mathbb{N}$ and $r \in 0 \ldots \ell - 1$. As $\ell = \mathrm{ord}(\sigma)$ we have $\sigma^\ell = \mathbb{1}$ such that we are enabled to compute

$$\sigma^k(i) \ = \ \sigma^{m\ell+r}(i) \ = \ \left(\sigma^\ell\right)^m \sigma^r(i) \ = \ \mathbb{1}^m\sigma^r(i) \ = \ \sigma^r(i)$$

Hence any $\sigma^k(i)$ is contained in $\{\sigma^r(i) \mid r \in 0 \dots \ell - 1\}$ such that we get $\mathrm{dom}(\sigma) = \{\sigma^r(i) \mid r \in 0 \dots \ell - 1\}$ due to the assumption (d).

- (e) $\implies$ (a): let us take $i_k := \sigma^{k-1}(i)$ for any $k \in 1 \dots \ell$. We first prove that there elements are truly pairwise distinct: Suppose $i_r = i_s$ for some $r \neq s$, without loss of generality we can take $r < s$. Then $\sigma^{r-1}(i) = \sigma^{s-1}(i)$ implies $\sigma^{s-r}(i) = i$ (by multiplication with σ^{1-r} from the left). That is there would have to be some $h = s - r \in \mathbb{N}$ with $\sigma^h(i) = i$. Thereby $h = s - r < s \leq \ell$ such that $h \in 1 \dots \ell - 1$. As $\ell = \mathrm{ord}(\sigma)$ is the minimal number with $\sigma^\ell = \mathbb{1}$ this implies $\sigma^h \neq \mathbb{1}$, that is there has to be some $a \in 1 \dots n$ with $\sigma^h(a) \neq a$. In particular $a \in \mathrm{dom}(\sigma)$ as else we would also have $\sigma^h(a) = a$. By assumption there hence is some $k \in 0 \dots \ell - 1$ such that $a = \sigma^k(i)$. Now compute
$$\sigma^h(a) \;=\; \sigma^h\sigma^k(i) \;=\; \sigma^k\sigma^h(i) \;=\; \sigma^k(i) \;=\; a$$
in contradiction to $\sigma^h(a) \neq a$. Hence the assumption $i_r = i_s$ must have been false, that is the i_k are pairwise distict. Hence we are entitled to define $\zeta := (i_1\ i_2\ \dots\ i_\ell)$. Then for any $k \in 1 \dots \ell - 1$ it is clear that $\zeta(i_k) = i_{k+1} = \sigma^k(i) = \sigma(\sigma^{k-1}(i)) = \sigma(i_k)$. However we also find $\zeta(i_\ell) = i_1 = i = \sigma^\ell(i) = \sigma(\sigma^{\ell-1}(i)) = \sigma(i_\ell)$. That is we have shown that $\zeta(a) = \sigma(a)$ for any $a \in \mathrm{dom}(\zeta)$. But as
$$\mathrm{dom}(\zeta) \;=\; \{\, i_1, i_2, \dots, i_\ell \,\} \;=\; \Big\{\, \sigma^k(i) \mid k \in 0 \dots \ell - 1 \,\Big\} \;=\; \mathrm{dom}(\sigma)$$
is true by assumption, this implies $\zeta = \sigma$. That is we have shown that σ truly is the cycle generated by the i_k.
- The fact that $\ell = \mathrm{ord}(\sigma)$ can be easily seen directly. But the implication (a) $\implies$ (e) already yields $\mathrm{ord}(\sigma) = \ell$, as the length ℓ of the cycle appears in (e) as the order of σ, since $\sigma^{k-1}(i) = i_k$.

□

Proof of (1.18):

(i) Let us abbreviate $X := 1 \dots n$ and $S := \big\{\, \sigma^k \mid k \in \mathbb{Z} \,\big\}$. Then this proof could be abbreviated by noting that $S \times X \to X : (\sigma, i) \mapsto \sigma(i)$ is a group action with the orbits $Si = \mathrm{cyc}(\sigma, i)$. Anyhow we want to give a direct proof that does not require group actions:

Clearly $\sim$ is an equivalence relation, $i \sim i$ is true, due to $i = \sigma^0(i)$ and if $i \sim j$ with $j = \sigma^p(i)$ and $j \sim k$ with $k = \sigma^q(j)$ then clearly $k = \sigma^q(\sigma^p(i)) = \sigma^{p+q}(i)$ such that $i \sim k$ again. Also let $z := \mathrm{ord}(\sigma) \in \mathbb{N}$ (also see (i)), then $\sigma^z = \mathbb{1}$ such that $(\sigma^k)^{-1} = \sigma^{-k} = \sigma^z\sigma^{-k} = \sigma^{z-k}$. Hence if $i \sim j$ with $j = \sigma^k(i)$ then $i = \sigma^{z-k}(j)$ such that $j \sim i$ again. And the equivalence class is obviously given to be
$$[i] \;=\; \{\, j \in X \mid j \sim i \,\} \;=\; \Big\{\, \sigma^k(i) \mid k \in \mathbb{N} \,\Big\} \;=\; \mathrm{cyc}(\sigma, i)$$
If now $j \in \mathrm{cyc}(\sigma, i)$, then j is of the form $j = \sigma^k(i)$ for some $k \in \mathbb{N}$. In particular $\sigma(j) = \sigma^{k+1}(i) \in \mathrm{cyc}(\sigma, i)$ again. And hence we get a well-defined map
$$\zeta_i \;:\; \mathrm{cyc}(\sigma, i) \;\hookrightarrow\; \mathrm{cyc}(\sigma, i) \;:\; a \mapsto \sigma(a)$$
Once more, as σ is injective and $\mathrm{cyc}(\sigma, i)$ is a finite set we even get $\sigma(\mathrm{cyc}(\sigma, i)) = \mathrm{cyc}(\sigma, i)$ such that the above ζ_i bocomes bijective. We now expand ζ_i to $1 \dots n$ trivially by letting $\zeta_i(a) := a$ for

any $a \notin \mathrm{cyc}(\sigma, i)$. Then it is clear, that

$$\mathrm{dom}(\zeta_i) \;=\; \mathrm{cyc}(\sigma, i)$$

And as ζ_i acts on $\mathrm{cyc}(\sigma,i) = \left\{ i, \sigma(i), \ldots, \sigma^{k(i)}(i) \right\}$ just like σ does, it also is clear, that $\zeta_i = (i\ \sigma(i)\ \ldots\ \sigma^{k(i)}(i))$. Now, as $\sim$ restricts to an equivanlence relation on $\mathrm{dom}(\sigma)$ [for $a \in \mathrm{fix}(\sigma)$ the equivalence class is just $[a] = \{ a \}$] we may pick up a system of representatives $i(1), \ldots, i(r)$. As the cycles are disjoint $\mathrm{cyc}(\sigma, i(p)) \cap \mathrm{cyc}(\sigma, i(q)) = \emptyset$ for $p \neq q \in 1 \ldots r$ we find from (1.14.(iv)) that the respective cycles commute

$$p \neq q \;\in\; 1 \ldots r \quad \Longrightarrow \quad \zeta_{i(p)} \zeta_{i(q)} \;=\; \zeta_{i(q)} \zeta_{i(p)}$$

Also if $a \in \mathrm{dom}(\sigma)$ then there is precisely one $p \in 1 \ldots r$ such that $a \in \mathrm{cyc}(\sigma, i(p)) = \mathrm{dom}(\zeta_{i(p)})$. In particular we have $a \in \mathrm{fix}(\zeta_{i(q)})$ for any $q \neq p$. And hence we get

$$\left(\prod_{j=1}^{r} \zeta_{i(j)} \right)(a) \;=\; \zeta_{i(p)} \prod_{q \neq p} \zeta_{i(q)}(a) \;=\; \zeta_{i(p)}(a) \;=\; \sigma(a)$$

Thereby we only used the fact, that we can bring $\zeta_{i(p)}$ in front by successively interchanging two cycles (which is obvious by induction on r). And if $a \in \mathrm{fix}(\sigma)$ then by consruction we also have $a \in \mathrm{fix}(\zeta_{i(p)})$ for any $p \in 1 \ldots r$ such that $(\zeta_{i(1)} \ldots \zeta_{i(r)})(a) = a = \sigma(a)$. In any case we have found $\sigma(a) = (\zeta_{i(1)} \ldots \zeta_{i(r)})(a)$ such that the equality $\sigma = \zeta_{i(1)} \ldots \zeta_{i(r)}$ is finally established, as well.

(ii) Let us abbreviate $\zeta := \zeta_1 \ldots \zeta_k$ and $\xi := \xi_1 \ldots \xi_t$. We will prove this statement by induction on $m := \min\{ k, t \}$. For $m = 1$ we already have $\zeta_1 = \xi_1$ such that there is nothing to prove. For $m \geq 2$ consider any $a \in \mathrm{dom}(\zeta_1)$. By assumption this implies $a \notin \mathrm{dom}(\zeta_i)$ for any $i \neq 1$. Hence we get

$$\zeta(a) \;:=\; \zeta_1 \ldots \zeta_k(a) \;=\; \zeta_1(a)$$

In particular $a \in \mathrm{dom}(\zeta) = \mathrm{dom}(\xi)$. Likewise there is a uniquely determined $r \in 1 \ldots t$ such that $a \in \mathrm{dom}(\xi_r)$ as for any $s \neq r$ we get $a \notin \mathrm{dom}(\xi_s)$. Hence - by (ii) - we have $\xi_r(a) \in \mathrm{dom}(\xi_r)$ again such that $\xi_r(a) \notin \mathrm{dom}(\xi_s)$ for any $s \neq r$, as well. This implies

$$\xi(a) \;:=\; \xi_1 \ldots \xi_t(a) \;=\; \xi_r(a)$$

Altogether $\zeta_1(a) = \zeta(a) = \xi(a) = \xi_r(a)$. We will now prove $\mathrm{dom}(\zeta_1) = \mathrm{dom}(\xi_r)$: given any $b \in \mathrm{dom}(\zeta_1)$ there is some $p \in \mathbb{N}$ such that $b = \zeta_1^p(a)$ by virtue of (1.17.(b)), as ζ_1 is a cycle. Therefore $b = \zeta_1^p(a) = \xi_r^p(a) \in \mathrm{dom}(\xi_r)$ by (ii) again. Altogether this is

$$\mathrm{dom}(\zeta_1) \quad \subseteq \quad \mathrm{dom}(\xi_r)$$

Reversing the roles of ζ_1 and ξ_r we find the converse inclusion, such that the domains are equal. In particular, given any $a \in \mathrm{dom}(\zeta_1)$ we can repeat the above calculation, to find

$$\forall\, a \in \mathrm{dom}(\zeta_1) = \mathrm{dom}(\xi_r) \;:\; \zeta_1(a) \;=\; \xi_r(a)$$

Clearly this implies $\zeta_1 = \xi_r$. Recall that the domains of the ξ_s were assumed to be pairwise disjoint, such that by (1.14.(iv)) the ξ_s are mutually commutative. Then we can compute

$$\zeta_2 \dots \zeta_k \;=\; \zeta_1^{-1}\zeta \;=\; \xi_r^{-1}\xi \;=\; \prod_{s\neq r} \xi_s$$

Hence by induction hypotheseis we find $k-1 = t-1$ and some permutation α such that $\zeta_i = \xi_{\alpha(i)}$ for any $i \in 2 \dots k$. Clearly this implies $k = t$ and we can append α to $\alpha \in S_r$ by $\alpha(1) := r$.

(iii) By (iv) σ can be written as a composition of cycles $\zeta_j := \zeta_{i(j)}$ with pairwise disjoint domains. And by (v) these cycles are uniquely determined. Hence this item (vi) is an immediate result of (iv) and (v).

(iv) By (iv) any permutation $\sigma \in S_n$ can be written as a composition of cycles $\sigma = \zeta_1 \dots \zeta_r$. And according to (1.16) any cycle ζ_i can be written as a composition of transpositions

$$\zeta_i \;=\; \prod_{j\in J(i)} \tau_{i,j}$$

Again, according to (1.16), any transposition $\tau_{i,j}$ can be written as a composition of adjacent transpositions

$$\tau_{i,j} \;=\; \prod_{k\in K(i,j)} \alpha_{i,j,k}$$

Altogether we can decompose σ into a - admittably *very* large - composition of adjacent cycles $\alpha_{i,j,k}$ by putting all this together.

(v) The implication (b) $\implies$ (a) is quite easy: pick up the cyclic decomposition $\varrho = \zeta_1 \dots \zeta_k$ as in (iii) and let $\xi_i := \pi\zeta_i\pi^{-1}$ for any $i \in 1 \dots r$. Then by (1.16) ξ_i is a cycle of the same length $\mathrm{ord}(\xi_i) = \mathrm{ord}(\zeta_i)$ again. And as π is bijective the cycles ξ_i are pairwise disjoint again. Now compute

$$\begin{aligned}\sigma \;&=\; \pi\varrho\pi^{-1} \;=\; \pi\zeta_1\zeta_2 \dots \zeta_k\pi^{-1}\\ &=\; \pi\zeta_1\pi^{-1}\pi\zeta_2\pi^{-1} \dots \pi\zeta_k\pi^{-1}\\ &=\; \xi_1\xi_2 \dots \xi_k\end{aligned}$$

That is we have found a cyclic decomposition of σ again. And by construction this decomposition satisfies the properties of (a). But as the cyclic decomposition of σ is unique (up to sequence, as we have seen in (ii)) (a) is true for *any* cyclic decomposition of σ.

The converse implication (a) $\implies$ (b) only requires little more effort: Let us abbreviate $\ell(i) := \mathrm{ord}(\zeta_i)$ the length of ζ_i. That is there are some numbers $a_{i,j} \in 1 \dots n$ such that ζ_i can be written as

$$\zeta_i \;=\; (a_{i,1}\;\; a_{i,2}\;\; \dots\;\; a_{i,\ell(i)})$$

And by assumption we have $\mathrm{ord}(\xi_{\alpha(i)}) = \mathrm{ord}(\zeta_i) = \ell(i)$ such that there also are numbers $b_{i,j} \in 1 \dots n$ such that $\xi_{\alpha(i)}$ can be written as

$$\xi_{\alpha(i)} \;=\; (b_{i,1}\;\; b_{i,2}\;\; \dots\;\; b_{i,\ell(i)})$$

As the domains of the ζ_i and the ξ_r are pairwise disjoint we obtain a disjoint union of sets (that compose the domain of ϱ)

$$D \;:=\; \bigcup_{i=1}^{k} \{\, a_{i,j} \mid j \in 1 \dots \ell(i) \,\}$$

And this enables us to define a permutation $\pi \in S_n$ by letting $\pi(a_{i,j}) := b_{i,j}$ for any $i \in 1 \dots k$ and $j \in 1 \dots \ell(i)$ and $\pi(a) := a$ for any $a \notin D$. Then by (1.16) it is clear that

$$\begin{aligned} \pi\zeta_i\pi^{-1} &= \pi(a_{i,1}\ a_{i,2}\ \dots\ a_{i,\ell(i)})\pi^{-1} \\ &= (\pi(a_{i,1})\ \pi(a_{i,2})\ \dots\ \pi(a_{i,\ell(i)})) \\ &= (b_{i,1}\ b_{i,2}\ \dots\ b_{i,\ell(i)}) \;=\; \xi_{\alpha(i)} \end{aligned}$$

Hence we find (reversing the computation in the case (b) $\Longrightarrow$ (a) above) that σ and ϱ are truly conjugates under π

$$\pi\varrho\pi^{-1} \;=\; \pi\left(\prod_{i=1}^{k}\zeta_i\right)\pi^{-1} \;=\; \prod_{i=1}^{k}(\pi\zeta_i\pi^{-1}) \;=\; \prod_{i=1}^{k}\xi_i \;=\; \sigma$$

□

Proof of (1.2) (commutativity):
We will now prove that in a commutative groupoid $(G, \circ)$ the order in which the elements $x_1, \dots, x_n \in G$ are multiplied has no impact on the result of the composition. That is for any permutation $\sigma \in S_n$ we have

$$x_{\sigma(1)}x_{\sigma(2)}\dots x_{\sigma(n)} \;=\; x_1x_2\dots x_n$$

As we have seen in (1.18.(iv)) any permutation $\sigma \in S_n$ can be expressed as a composition of adjacent transpositions

$$\sigma \;=\; \alpha_1\,\alpha_2\,\dots\,\alpha_s$$

We will now prove the claim by induction on the number of transpositions s. In case $s = 1$ we have to deal with one adjacent transposition, say $\alpha = (j\ j+1)$. Then we have

$$\prod_{i=1}^{n} x_{\alpha(i)} \;=\; x_1\dots x_{j-1}\,x_{j+1}\,x_j\,x_{j+2}\dots x_n$$

But by the commutativity rule (C) we can interchange x_{j+1} and x_j in this product to find $x_{\alpha(1)}x_{\alpha(2)}\dots x_{\alpha(n)} = x_1\dots x_jx_{j+1}\dots x_n$. In case $s \geq 2$ we let $\alpha := \alpha_1$ and $\varrho = \alpha_2\dots\alpha_s$. Then it is clear that $\sigma = \alpha\varrho$. And as in the case $s = 1$ resp. by induction hypothesis we get

$$\prod_{i=1}^{n} x_{\sigma(i)} \;=\; \prod_{i=1}^{n} x_{\alpha\varrho(i)} \;=\; \prod_{i=1}^{n} x_{\varrho(i)} \;=\; \prod_{i=1}^{n} x_i$$

□

Proof of (1.22):

(i) Let us denote the set $\Delta := \{(i,j) \in (1\dots n)^2 \mid i < j\}$ and the map $\delta : (1\dots n)^2 \to \mathbb{Z} : (i,j) \mapsto j - i$.

For $p, q \in \mathbb{N}$ we let $p \wedge q$ be the minimum and $p \vee q$ be the maximum of p and q. At last we define

$$\Sigma \;:\; \Delta \to \Delta \;:\; (i,j) \mapsto (\sigma(i) \wedge \sigma(j), \sigma(i) \vee \sigma(j))$$

Thereby Σ is well defined, since $1 \leq \sigma(i) \wedge \sigma(j) < \sigma(i) \vee \sigma(j) \leq n$. In fact Σ even is bijective, as we can explicitly give its inverse to be

$$\Sigma^{-1} \;:\; \Delta \to \Delta \;:\; (i,j) \mapsto (\sigma^{-1}(i) \wedge \sigma^{-1}(j), \sigma^{-1}(i) \vee \sigma^{-1}(j))$$

As Δ is finite it suffices to check $\Sigma^{-1}\Sigma = \mathbb{1}_\Delta$: let $(p,q) := \Sigma(i,j)$, then p and $q \in \{\, \sigma(i), \sigma(j) \,\}$ and $p < q$. Hence $\sigma^{-1}(p)$ and $\sigma^{-1}(q) \in \{\, i, j \,\}$, so ordering them we get $\Sigma^{-1}(p,q) = (i,j)$ again, which is the bijectivity of Σ. Also we easily compute

$$\begin{aligned} \delta\Sigma(i,j) &= \begin{cases} \sigma(j) - \sigma(i) \text{ if } \sigma(j) > \sigma(i) \\ \sigma(i) - \sigma(j) \text{ if } \sigma(j) < \sigma(i) \end{cases} \\ &= \big(\sigma(j) - \sigma(i)\big) \begin{cases} 1 \text{ if } \sigma(j) > \sigma(i) \\ -1 \text{ if } \sigma(j) < \sigma(i) \end{cases} \end{aligned}$$

After all these preparations we can proceed to the main computation: we use the fact that (due to the commutativity of $\mathbb{Z}$) the product can be permuted arbitrarily without changing its result. Here we have

$$\begin{aligned} \prod_{(i,j)\in\Delta} (j-i) &= \prod_{(i,j)\in\Delta} \delta(i,j) = \prod_{(p,q)\in\Sigma(\Delta)} \delta(i,j) \\ &= \prod_{(i,j)\in\Delta} \Sigma\delta(i,j) = (-1)^{I(\sigma)} \prod_{(i,j)\in\Delta} \big(\sigma(j) - \sigma(i)\big) \end{aligned}$$

And from here we are almost done, note that the product $\prod(j-i)$ is non-zero, as we always have $i < j$. Also $1/(-1)^{I(\sigma)} = (-1)^{I(\sigma)}$ as this number is either $+1$ or -1. Hence dividing by the product and $(-1)^{I(\sigma)}$ we finally get

$$(-1)^{I(\sigma)} = \frac{\prod_{(i,j)\in\Delta} \big(\sigma(j) - \sigma(i)\big)}{\prod_{(i,j)\in\Delta}(j-i)} = \prod_{(i,j)\in\Delta} \frac{\sigma(j) - \sigma(i)}{j-i}$$

(iv) Let us continue with the notation introduced in (i) above. Then we have already shown the following identity for any permutation σ

$$(-1)^{I(\sigma)} \prod_{(i,j)\in\Delta} (j-i) = \prod_{(i,j)\in\Delta} \big(\sigma(j) - \sigma(i)\big)$$

Using this identity for the composition $\varrho\sigma$ and the permutations σ and ϱ separately we can again compute

$$(-1)^{I(\varrho\sigma)} \prod_{(i,j)\in\Delta} (j-i) = \prod_{(i,j)\in\Delta} \big(\varrho\sigma(j) - \varrho\sigma(i)\big)$$

$$
\begin{aligned}
&= (-1)^{I(\sigma)} \prod_{(i,j)\in\Delta} \big(\varrho(j) - \varrho(i)\big) \\
&= (-1)^{I(\sigma)}(-1)^{I(\varrho)} \prod_{(i,j)\in\Delta} (j-i)
\end{aligned}
$$

Hence dividing by the product $\prod(j-i)$ we have established the homomorphism property of the signum, expressed in terms of (i):

$$
\begin{aligned}
\operatorname{sgn}(\varrho\sigma) &= (-1)^{I(\varrho\sigma)} = (-1)^{I(\sigma)}(-1)^{I(\varrho)} \\
&= (-1)^{I(\varrho)}(-1)^{I(\varrho)} = \operatorname{sgn}(\varrho)\operatorname{sgn}(\sigma)
\end{aligned}
$$

(iii) Consider the permutation $\tau = (a\ b)$ where (without loss of generality) $a < b$. Then it is easy to see, that τ has the following inversions

$$
\begin{aligned}
&\{\, (i,j) \in \Delta \mid \tau(i) > \tau(j) \,\} \\
&= \{\, (a, a+s) \mid 1 \le s \le b-a \,\} \cup \{\, (a+r, b) \mid 1 \le r < b-a \,\}
\end{aligned}
$$

In particular we get $I(\tau) = (b-a) + (b-a-1) = 2(b-a) - 1$ and thereby we get - using variant (i) of computing the signum

$$
\operatorname{sgn}(\tau) = (-1)^{I(\tau)} = (-1)^{2(b-a)-1} = \big((-1)^2\big)^{b-a}(-1)^{-1} = -1
$$

That is any transposition is an odd permutation! Thus, if $\sigma = \tau_1 \dots \tau_r$ is a composition of r transpositions, then the homomorphism property (iv) of the signum implies

$$
\operatorname{sgn}(\sigma) = \prod_{i=1}^{r} \operatorname{sgn}(\tau_i) = \prod_{i=1}^{r} (-1) = (-1)^r
$$

(ii) By (1.16) we know that any cycle ζ_i can be written as a composition of $\ell(i) - 1$ transpositions. Hence - by (iv) combined with (iii)

$$
\operatorname{sgn}(\sigma) = \operatorname{sgn}(\zeta_1 \dots \zeta_r) = \prod_{i=1}^{r} \operatorname{sgn}(\zeta_i) = \prod_{i=1}^{r} (-1)^{\ell(i)-1}
$$

And as the domains of the ζ_i are pairwise disjoint (1.14.(iv)) implies, that they are mutually commutative. Hence by (1.5) we find that any power $k \in \mathbb{N}$ of σ is just

$$
\sigma^k = \prod_{i=1}^{r} \zeta_i^k
$$

Also as $\operatorname{dom}(\zeta_i^k) \subseteq \operatorname{dom}(\zeta_i)$ (this is (1.14.(ii))) and the $\operatorname{dom}(\zeta_i)$ are pairwise disjoint we have (for any $a \in 1 \dots n$) $\sigma(a) = a$ if and only if $\zeta_i^k(a) = a$ for any $i \in 1 \dots r$. In particular we see the equivalence of

$$
\sigma^k = \mathbb{1} \iff \forall\, i \in 1 \dots r : \zeta_i^k = \mathbb{1}
$$

As ζ_i is a cycle its order is given to be $\ell(i) = \operatorname{ord}(v_i)$. Hence $\zeta_i^k = \mathbb{1}$ if and only if $\ell(i)$ divides k (by division with remainder again, write $k = m\ell(i) + r$ then $\zeta_i^k = (\zeta_i^{\ell(i)})^m \zeta_i^r = \zeta_i^r = \mathbb{1}$ iff $r = 0$).

Therefore

$$\sigma^k \;=\; \mathbb{1} \quad\Longleftrightarrow\quad \forall\, i \in 1 \dots r \;:\; \ell(i) \;\mid\; k$$

Now $\operatorname{ord}(\sigma) = k$ is the minimal number $1 \leq k \in \mathbb{N}$ such that $\sigma^k = \mathbb{1}$. And likewise $\operatorname{lcm}(\ell(1), \dots, \ell(r))$ is the minimal number that is divided, by all the $\ell(i)$. In particular both numbers are equal.

(v) By definition A_n is just the kernel of the group-homomorphism $\operatorname{sgn} : S_n \to \mathbb{Z}^*$. Therefore the first isomorphism theorem (of groups) yields

$$S_n \Big/ A_n \;\xrightarrow{\sim}\; \mathbb{Z}^* \;:\; \sigma A_n \mapsto \operatorname{sgn}(\sigma)$$

In particular these two sets have the same cardinality. Now use the theorem of Lagrange and (1.12.(i)) to compute

$$2 \;=\; \#\mathbb{Z}^* \;=\; \#S_n \Big/ \#A_n \;=\; \frac{\#S_n}{\#A_n} \;=\; \frac{n!}{\#A_n}$$

□

Proof of (1.29):

- The properties of ι are clear. Also it is straightforward to see, that for any $b \in \mathbb{Z}$ and $y \in S$ we have $(0,0) + (b,y) = (b,y)$ and $(1,0) \cdot (b,y) = (b,y)$ and likewise $(b,y) \cdot (1,0) = (b,y)$. Thus $(0,0)$ is the zero-element and $(1,0)$ the unit element of R. Also it can be checked without effort, that $(R,+)$ is a commutative group, as both $(\mathbb{Z},+)$ and $(S,+)$ are.

- In the next step we prove that S becomes a $\mathbb{Z}$-module under its own addition and the following scalar-multiplication: For any $x \in S$ and any $a \in \mathbb{Z}$ we define $ax \in S$ by distinguishing three cases: (1) If $a = 0$ then $ax := 0$, (2) If $a > 0$ we define $ax := x + x + \dots + x$ (a-times) and (3) If $a < 0$ and $\alpha := -a > 0$ we define $ax := (-x) + (-x) + \dots (-x)$ (α-times). Actually case (1) can be considered a sub-case of (2). Also we have defined $ax := (-\alpha)(-x)$, so actually (2) is the one and only relevant case, (3) can be reduced to (2). From this definition it is clear, that $1x = x$ and $(a+b)x = (ax) + (bx)$ already. Also $a(x+y) = (ax) + (ay)$ is plain to see, as $+$ is commutative. Now take a look at $a(bx) = bx + bx + \dots + bx$ (a-times). If we just write out $bx = x + x + \dots + x$ all the time, we see, that $a(bx)$ is the sum of ab-times x, this is it equals $a(bx) = (ab)x$. This is the last property we needed, for a $\mathbb{Z}$-module.

- With these properties at hand we may prove the distributivity rules for R: Consider any a, b, $c \in \mathbb{Z}$ and x, y, $z \in S$. For the sake of clarity let us write the tuples (a,x) as column vectors, instead, then we compute:

$$\begin{aligned}
\begin{pmatrix} a \\ x \end{pmatrix} \left(\begin{pmatrix} b \\ y \end{pmatrix} + \begin{pmatrix} c \\ z \end{pmatrix} \right) \;&=\; \begin{pmatrix} a \\ x \end{pmatrix} \begin{pmatrix} b+c \\ y+z \end{pmatrix} \\
&=\; \begin{pmatrix} a(b+c) \\ a(y+z) + (b+c)x + x(y+z) \end{pmatrix} \\
&=\; \begin{pmatrix} ab+ac \\ ay+az+bx+cx+xy+xz \end{pmatrix} \\
\begin{pmatrix} a \\ x \end{pmatrix} \begin{pmatrix} b \\ y \end{pmatrix} + \begin{pmatrix} a \\ x \end{pmatrix} \begin{pmatrix} c \\ z \end{pmatrix} \;&=\; \begin{pmatrix} ab \\ ay+bx+xy \end{pmatrix} \begin{pmatrix} ac \\ az+cx+xz \end{pmatrix}
\end{aligned}$$

$$= \begin{pmatrix} ab+ac \\ ay+bx+xy+az+cx+xy \end{pmatrix}$$

We just need to rearrange these 6 terms a little, which is allowed, since the addition on S is commutative, to find the identity of these expressions. So this is the distributivity rule of multiplication from the left. Multiplication from the right can be done in precisely the same way.

- Before we continue, we need another preliminary: Any semi-ring is a $\mathbb{Z}$-semi-algebra under its own multiplication and the scalar-multiplication introduced above. We have to verify the three compatibility properties (A) of the multiplication with the scalar-multiplication. We begin with $a \geq 0$ and $x, y \in S$. Then we compute $x(ay) = x(y+y+\cdots+y) = (xy+xy+\cdots+xy) = a(xy)$. That is we have verified the associativity $a(xy) = x(ay)$ for $a \in \mathbb{N}$. For $a < 0$ we have let $\alpha := -a \in \mathbb{N}$, then $ay = (-\alpha)(-y)$ and hence $x(ay) = x((-\alpha)(-y)) = (-\alpha)(x(-y)) = (-\alpha)(-xy) = a(xy)$. Thus we generally have $a(xy) = x(ay)$ for any $a \in \mathbb{Z}$. In exactly the same way, we see that $(ax)y = a(xy)$ for any $a \in \mathbb{Z}$ and $x, y \in S$. Let us summarize:

$$(ax)y \;=\; a(xy) \;=\; x(ay)$$

As with the associativity $(xy)z = x(yz)$ it is customary to omit the brackets in $(ax)y = a(xy)$, as both terms yield the same result. We will need these identities and $a(bx))(ab)x$ in the next step.

- It remains to check that the multiplication on R truly satisfies the properties of a ring: associativity, distributivity. Thus we start with a, b and $c \in \mathbb{Z}$ and x, y, $z \in S$ and head out for a series of computations:

$$\begin{aligned}
\left(\begin{pmatrix} a \\ x \end{pmatrix}\begin{pmatrix} b \\ y \end{pmatrix}\right)\begin{pmatrix} c \\ z \end{pmatrix} &= \begin{pmatrix} ab \\ ay+bx+xy \end{pmatrix}\begin{pmatrix} c \\ z \end{pmatrix} \\
&= \begin{pmatrix} abc \\ (ab)z+c(ay)+c(bx)+c(xy)+(ay)z+(bx)z+(xy)z \end{pmatrix} \\
&= \begin{pmatrix} abc \\ abz+cay+cbx+cxy+ayz+bxz+xyz \end{pmatrix} \\
\begin{pmatrix} a \\ x \end{pmatrix}\left(\begin{pmatrix} b \\ y \end{pmatrix}\begin{pmatrix} c \\ z \end{pmatrix}\right) &= \begin{pmatrix} a \\ x \end{pmatrix}\begin{pmatrix} bc \\ bz+cy+yz \end{pmatrix} \\
&= \begin{pmatrix} abc \\ a(bz)+a(cy)+a(yz)+(bc)x+x(bz)+x(cy)+x(yz) \end{pmatrix} \\
&= \begin{pmatrix} abc \\ abz+acy+ayz+bcx+bxz+cxy+xyz \end{pmatrix}
\end{aligned}$$

As the multiplication in $\mathbb{Z}$ is commutative we have $cay = acy$ and $cbx = bcx$. Therefore both of these expressions contain exactly the same 7 terms. And as the addition on S is commutative, we find that the sums are equal. This is the associativity of R.

□

Proof of (1.41):

- The statement $0 = -0$ is clear from $0+0=0$. And $a0 = 0$ follows from $a0 = a(0+0) = a0 + a0$. Likewise we get $0a = 0$. And from this an easy computation shows $(-a)b = -(ab)$, this computation reads as $ab + (-a)b = (a + (-a))b = 0b = 0$ (and $a(-b) = -(ab)$ follows analogously). Combining these two we find $(-a)(-b) = ab$, since $ab = -(-ab) = -((-a)b) = (-a)(-b)$.

- Next we will prove the general rule of distributivity: we start by showing that $(a_1 + \cdots + a_m)b = (a_1 b) + \cdots + (a_m b)$ by induction on m. The case $m = 1$ is clear and in the induction step we simply compute

$$\begin{aligned}\Big(a_1 + \cdots + a_m + a_{m+1}\Big)\, b &= \Big((a_1 + \cdots + a_m) + a_{m+1}\Big)\, b \\ = \left(\sum_{i=1}^{m} a_i\right) b + a_{m+1}b &= \left(\sum_{i=1}^{m} a_i b\right) + a_{m+1}b = \sum_{i=1}^{m+1} a_i b\end{aligned}$$

 Likewise it is clear, that $a(b_1 + \cdots + b_n) = (ab_1) + \cdots + (ab_n)$. And combining these two equations we find the generale rule

$$\begin{aligned}\left(\sum_{i=1}^{m} a_i\right)\left(\sum_{j=1}^{n} b_j\right) &= \sum_{j=1}^{n}\left(\sum_{i=1}^{m} a_i\right) b_j \\ &= \sum_{j=1}^{n}\left(\sum_{i=1}^{m} a_i b_j\right) \\ &= \sum_{i=1}^{m}\sum_{j=1}^{n} a_i b_j\end{aligned}$$

- Using induction on n we will now prove the generalization of the general law of distributivity. The case $n = 1$ is trivial (here $J = J(1)$ so there is nothing to prove). Thus consider the induction step by adding $J(0)$ to our list $J(1), \ldots, J(n)$ of index sets. Then clearly

$$\prod_{i=0}^{n}\sum_{j_i \in J(i)} a(i, j_i) = \left(\sum_{j_0 \in J(0)} a(0, j_0)\right)\left(\prod_{i=1}^{n}\sum_{j_i \in J(i)} a(i, j_i)\right)$$

 Hence we may use the induction hypothesis in the second term on the right hand side and the general law of distributivity (note that we use $J = J(1) \times \cdots \times J(n)$) again) to obtain

$$\begin{aligned}\prod_{i=0}^{n}\sum_{j_i \in J(i)} a(i, j_i) &= \left(\sum_{j_0 \in J(0)} a(0, j_0)\right)\left(\sum_{j \in J}\prod_{i=1}^{n} a_{i,j_i}\right) \\ &= \sum_{j_0 \in J(0)}\sum_{j \in J} a(0, j_0)\prod_{i=1}^{n} a(i, j_i)\end{aligned}$$

 To finish the induction step it suffices to note that the product of $a(0, j_0)$ with $\prod_{i=1}^{n} a(i, j_i)$ can be rewritten $\prod_{i=0}^{n} a(i, j_i)$ (due to the associativity of the multiplication). And the two sums over $j(0) \in J(0)$ resp. over $j \in J$ can be composed to a single sum over $(j_0, j) \in J(0) \times J$. Thas is we

have obtained the claim

$$\prod_{i=0}^{n} \sum_{j_i \in J(i)} a(i,j_i) \;=\; \sum_{(j_0,j)\in J(0)\times J} \prod_{i=0}^{n} a(i,j_i)$$

- Thus we have arrived at the binomial rule, which will be proved by induction on n. In the case $n=0$ we have $(a+b)^0 = 1 = 1\cdot 1 = a^0 b^{0-0}$. Thus we commence with the induction step

$$\begin{aligned}
& (a+b)^{n+1} \;=\; (a+b)^n (a+b) \\
=\;& \left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \right) (a+b) \\
=\;& \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{(n+1)-k} \\
=\;& \sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{(n+1)-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{(n+1)-k} \\
=\;& \binom{n}{n} a^{n+1} b^0 + \sum_{k=1}^{n} \left(\binom{n}{k-1} + \binom{n}{k} \right) a^k b^{(n+1)-k} + \binom{n}{0} a^0 b^{n+1} \\
=\;& \binom{n+1}{0} a^0 b^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^k b^{(n+1)-k} + \binom{n+1}{n+1} a^{n+1} b^0 \\
=\;& \sum_{k=0}^{n+1} \binom{n}{k} a^k b^{n-k}
\end{aligned}$$

- It remains to verify the polynomial rule, which will be done by induction on k. The case $k=1$ is clear again, and the case $k=2$ is the ordinary binomial rule. Thus consider the induction step

$$\begin{aligned}
& \Big(a_1 + \cdots + a_k + a_{k+1} \Big)^n \\
=\;& \Big(a_{k+1} + (a_1 + \cdots + a_k) \Big)^n \\
=\;& \sum_{\alpha_{k+1}=0}^{n} \binom{n}{\alpha_{k+1}} a_{k+1}^{\alpha_{k+1}} (a_1 + \cdots + a_k)^{n-\alpha_{k+1}} \\
=\;& \sum_{\alpha_{k+1}=0}^{n} \binom{n}{\alpha_{k+1}} a_{k+1}^{\alpha_{k+1}} \left(\sum_{|\alpha|=n-\alpha_{k+1}} \binom{n-\alpha_{k+1}}{\alpha} a^\alpha \right) \\
=\;& \sum_{\alpha_{k+1}=0}^{n} \sum_{|\alpha|=n-\alpha_{k+1}} \binom{n}{\alpha_{k+1}} \binom{n-\alpha_{k+1}}{\alpha} a^\alpha a_{k+1}^{\alpha_{k+1}} \\
=\;& \sum_{|(\alpha,\alpha_{k+1})|=n} \binom{n}{(\alpha,\alpha_{k+1})} (a, a_{k+1})^{(\alpha,\alpha_{k+1})}
\end{aligned}$$

□

Proof of (1.44):
Let us regard the polynomial ring $R = \mathbb{Z}[x,y]$ in two variables x and y. As R is commutative it is clear,

that $(x+y)^n = (x+y)^k(x+y)^{n-k}$. By the binomial rule (1.41) we may evaluate these terms to

$$\begin{aligned}\sum_{r=0}^{n}\binom{n}{r}x^r y^{n-r} &= \left(\sum_{i=0}^{k}\binom{k}{i}x^i y^{k-i}\right)\left(\sum_{j=0}^{n-k}\binom{n-k}{j}x^j y^{n-k-j}\right)\\ &= \sum_{r=0}^{n}\sum_{i+j=r}\binom{k}{i}\binom{n-k}{j}x^{i+j}y^{k-i+n-k-j}\\ &= \sum_{r=0}^{n}\sum_{i+j=r}\binom{k}{i}\binom{n-k}{j}x^r y^{n-r}\end{aligned}$$

where we also used the general rule of distributivity. Now we may compare coefficients (which is allowed by construction of R) to find our claim (as $j = r - i$)

$$\binom{n}{r} = \sum_{i+j=r}\binom{k}{i}\binom{n-k}{j} = \sum_{i=0}^{r}\binom{k}{i}\binom{n-k}{r-i}$$

□

Proof of (1.45):

We now prove the equivalences for integral rings: For (a) $\implies$ (b') we are given a, b and $c \in R$ with $a \neq 0$ and $ba = ca$. Then we get $(c-b)a = 0$ which is $c - b \in \text{ZD}(R)$. By assumption (a) this implies $c - b = 0$ and hence $b = c$. Now the implication (b') $\implies$ (c') is trivial, just let $c = 1$. And for the final step (c') $\implies$ (a) we consider $0 \neq b \in R$ such that $ab = 0$. Then $(a+1)b = ab + b = b$ such that by assumption (c') we get $a + 1 = 1$ and hence $a = 0$. Thereby we have obtained $\text{ZD}(R) \subseteq \{0\}$ and the converse inclusion is clear.

Next we consider (a) $\implies$ (b), again we are given a, b and $c \in R$ with $a \neq 0$ and $ab = ac$. This yields $a(c-b) = 0$ and as $a \neq 0$ we have $a \notin \text{ZD}(R)$ such that $a \in \text{NZD}(R)$. Hence $c - b = 0$ which is $b = c$. The implication (b) $\implies$ (c) is clear again, just let $c = 1$. And for (c) $\implies$ (a) we consider $0 \neq a \in R$ such that $ab = 0$. Then $a(b+1) = ab + a = a$. By assumption (c) this implies $b + 1 = 1$ and hence $b = 0$. Therefore $R \setminus \{0\} \subseteq \text{NZD}(R)$ which is $R \setminus \{0\} = \text{NZD}(R)$ and hence $\text{ZD}(R) = \{0\}$. □

Proof of (1.47):

(i) The equality of sets $\text{NZD}(R) = R \setminus \text{ZD}(R)$ is immediately clear from the definition: The negation of the formula $\exists\, b \in R : (b \neq 0) \wedge (ab = 0)$ is just $\forall\, b \in R : ab = 0 \implies b = 0$.

(ii) If $a \in \text{NIL}(R)$ then we choose $k \in \mathbb{N}$ minimal such that $a^k = 0$. Suppose $k = 0$, then $0 = a^0 = 1$ which would mean that $R = 0$ has been the zero-ring. Thus we have $k \geq 1$ and may hence define $b := a^{k-1} \neq 0$. Then $ab = a^k = 0$ and hence $a \in \text{ZD}(R)$, which proves $\text{NIL}(R) \subseteq \text{ZD}(R)$. And if $ab = 0$, then $a \in R^{ast}$ would imply $b = a^{-1}0 = 0$. Thus if $a \in \text{ZD}(R)$ then $a \notin R^*$ which also proves $\text{ZD}(R) \subseteq R \setminus R^*$.

(iii) It is clear that $1 \in \text{NZD}(R)$, as $1b = b$. Now suppose a and $b \in \text{NZD}(R)$ and consider any $c \in R$. If $(ab)c = 0$ then (because of the associativity $a(bc) = 0$ and as $a \in \text{NZD}(R)$ this implies $bc = 0$. As $b \in \text{NZD}(R)$ this now implies $c = 0$ which means $ab \in \text{NZD}(R)$.

(iv) It is clear that $1 \in R^*$ - just choose $b = 1$. Now the associativity and existence of a neutral element $e = 1$ is immediately inherited from (the multiplication) of R. Thus consider $a \in R^*$, by definition

there is some $b \in R$ such that $ab = 1 = ba$. Hence we also have $b \in R^*$ and thereby b is the inverse element of a in R^*.

(v) " $\Longleftarrow$ " first suppose $0 = 1 \in R$ then we would have $R = 0$ and hence $R \setminus \{0\} = \emptyset$ and $R^* = R \neq \emptyset$, in contradiction to the assumption $R^* = R \setminus \{0\}$. Thus we get $0 \neq 0$. If now $0 \neq a \in R$ then $a \in R^*$ by assumption and hence there is some $b \in R$ such that $ab = 1 = ba$. But this also is property (F) of skew-fields. " $\Longrightarrow$ " if $0 \neq a \in R$ then - as R is a skew field - there is some $b \in R$ such that $ab = 1 = ba$. But this already is $a \in R^*$ and hence $R \setminus \{0\} \subseteq R^*$. Conversely consider $a \in R^*$, that is $ab = 1 = ba$ for some $b \in R$. Suppose $a = 0$, then $1 = ab = 0 \cdot b = 0$ and hence $0 = 1$, a contradiction. Thus $a \neq 0$ and this also proves $R^* \subseteq R \setminus \{0\}$.

(vi) Consider a and $b \in \text{NIL}(R)$ such that $a^k = 0$ and $b^l = 0$. Then we will prove $a + b \in \text{NIL}(R)$ by demonstrating $(a+b)^{k+l} = 0$, via

$$\begin{aligned}
(a+b)^{k+l} &= \sum_{i=0}^{k+l} \binom{k+l}{i} a^i b^{k+l-i} \\
&= \sum_{i=0}^{k} \binom{k+l}{i} a^i b^{l+(k-i)} + \sum_{j=1}^{l} \binom{k+l}{k+j} a^{k+j} b^{l-j} \\
&= b^l \sum_{i=0}^{k} \binom{k+l}{i} a^i b^{k-i} + a^k \sum_{j=1}^{l} \binom{k+l}{k+j} a^j b^{l-j} \\
&= 0 + 0 \;=\; 0
\end{aligned}$$

And if $c \in R$ is an arbitrary element, then also $(ca)^k = c^k a^k = c^k 0 = 0$ such that $ca \in \text{NIL}(R)$. As a has been chosen arbitarily, this implies $R\,(\text{NIL}(R)) \subseteq R$ and hence $\text{NIL}(R) \trianglelefteq_{\text{i}} R$ is an ideal.

(vii) Consider x and $y \in \text{ann}(b)$. Then it is clear that $(x+y)b = xb + yb = 0 + 0 = 0$ and hence $x + y \in \text{ann}(b)$. And if $a \in R$ is arbitrary then $(ax)b = a(bx) = a0 = 0$ such that $ax \in \text{ann}(b)$. In particular $-x = (-1)x \in \text{ann}(b)$ and hence $\text{ann}(b)$ is a sub-module of R.

(viii) Let $u \in R^*$ and $a \in R$ with $a^n = 0$, then we can verify the formula for the inverse of $u + a$ in straightforward computation (see below). And in particular we found $u + a \in R^*$. But as a has been an arbitrary nilpotent, this has truly been $u + \text{NIL}(R) \subseteq R^*$.

$$\begin{aligned}
& (a+u) \sum_{k=0}^{n-1} (-1)^k a^k u^{-k-1} \\
= \;& \sum_{k=0}^{n-1} (-1)^k a^{k+1} u^{-(k+1)} + \sum_{k=0}^{n-1} (-1)^k a^k u^{-k} \\
= \;& \sum_{k=1}^{n} (-1)^{k-1} a^k u^{-k} \sum_{k=0}^{n-1} (-1)^k a^k u^{n-(k-1)} \\
= \;& (-1)^{n-1} a^n u^{-n} + (-1)^0 a^0 u^{-0} \;=\; 1
\end{aligned}$$

(ix) We identify R with the subset $\{\, a/1 \mid a \in R \,\} \subseteq F$. If $E = F$ then it is clear that $R \subseteq F = E$. Conversely suppose $R \subseteq E$, any $a/b \in F$ is composed of a, $b \in R$ with $b \neq 0$. As $R \subseteq E$ and $b \neq 0$ we have $b^{-1} \in E$ and therefore $a/b = ab^{-1} \in E$. But as this is true for any $a/b \in F$ we find $F \subseteq E$ and therefore $E = F$.

□

Proof of (1.52):

- ($\star$ = semi-ring) as any P_i is a sub-semiring we have $0 \in P_i$ and hence $0 \in \bigcap_i P_i$ again. Now consider $a, b \in \bigcap_i P_i$ that is $a, b \in P_i$ for any $i \in I$. As any P_i is a sub-semiring this implies that $a+b$, ab and $-a \in P_i$ (for any $i \in I$). And thereby $a+b$, ab and $-a \in \bigcap_i P_i$ again.

- ($\star =$ ring) in complete analogy we have $1 \in P_i$ (for any $i \in I$, as any P_i has been assumed to be a sub-ring. Hence we also get $1 \in \bigcap_i P_i$.

- ($\star =$ (skew)field) consider $0 \neq a \in \bigcap_i P_i$. That is $a \in P_i$ for any $i \in I$ and as any P_i is a subfield we get $a^{-1} \in P_i$ such that $a^{-1} \in \bigcap_i P_i$.

- ($\star =$ (left)ideal) consider any $b \in R$ and $a \in \bigcap_i P_i$ - that is $a \in P_i$ for any $i \in I$. As P_i is a left-ideal we find $ba_i \in P_i$ again and hence $ba \in \bigcap_i P_i$. In the case of ideals P_i we analogously find $ab \in \bigcap_i P_i$.

- Note that thereby the generation of $\star$ is well-defined - the set of all $\star$s containing X is non-empty, as R itself is a $\star$ (e.g. R is an ideal of R). And by the lemma we have just proved, the intersection is a $\star$ again.

□

Proof of (1.55):

- Let us denote the set $\mathfrak{a} := \{\sum_i a_i x_i\}$ of which we claim $\mathfrak{a} = \langle X \rangle_{\mathsf{m}}$. First of all it is clear that $X \subseteq \mathfrak{a}$, as $x = 1x \in \mathfrak{a}$ for any $x \in X$. Further it is clear that $\mathfrak{a} \leq_{\mathsf{m}} R$ is a left-ideal of R: choose any $x \in X$, then $0 = 0 \cdot x \in \mathfrak{a}$, and if $b \in R$, $x = a_1 x_1 + \cdots + a_m x_m$ and $y = b_1 y_1 + \cdots + b_n y_n \in \mathfrak{a}$ then $bx = (ba_1)x_1 + \cdots + (ba_m)x_m \in \mathfrak{a}$ and $x + y = a_1 x_1 + \cdots + a_m x_m + b_1 y_1 + \cdots + b_n y_n \in \mathfrak{a}$. Thus by definition of $\langle X \rangle_{\mathsf{m}}$ we get $\langle X \rangle_{\mathsf{m}} \subseteq \mathfrak{a}$. Now suppose $\mathfrak{b} \leq_{\mathsf{m}} R$ is any left-ideal of R containing $X \subseteq \mathfrak{b}$, Then for any $a_i \in R$ and any $x_i \in X \subseteq \mathfrak{b}$ we get $a_i x_i \in \mathfrak{b}$ and hence $\sum_i a_i x_i \in \mathfrak{b}$, too. That is $\mathfrak{a} \subseteq \mathfrak{b}$, and as $\mathfrak{b}$ has been arbitrary this means $\mathfrak{a} \subseteq \langle X \rangle_{\mathsf{m}}$, by the definition of $\langle X \rangle_{\mathsf{m}}$.

- Denote the set $P := \{\sum_i \prod_j x_{i,j}\}$ of which we claim $P = \langle X \rangle_{\mathsf{s}}$ again. Trivially we have $X \subseteq P$ and further it is clear that $P \leq_{\mathsf{s}} R$ is a sub-semi-algebra of R: choose any $x \in X$, then $0 = 0 \cdot x \in P$, and if $a = \sum_i \prod_j x_{i,j}$ and $b = \sum_k \prod_l y_{k,l}$, then $-a = \sum_i (-x_{i,1}) \prod_{j \geq 2} x_{i,j} \in P$, $a + b = \sum_i \prod_j x_{i,j} + \sum_k \prod_l y_{k,l} \in P$ and by general distributivity also $ab = \sum_i \sum_j (\prod_j x_{i,j} \prod_l y_{k,l}) \in P$. Thus by definition of $\langle X \rangle_{\mathsf{s}}$ we get $\langle X \rangle_{\mathsf{s}} \subseteq P$. Now suppose $Q \leq_{\mathsf{s}} R$ is any sub-semi-ring of R. Then for any and any $x \in X \subseteq Q$ we also get $-x \in Q$ and hence $\pm X \subseteq Q$. Now consider any $x_{i,j} \in \pm X \subseteq Q$ then $\prod_j x_{i,j} \in Q$ and hence $\prod_j x_{i,j} \in Q$. That is $P \subseteq Q$, and as Q has been arbitrary, this means $P \subseteq \langle X \rangle_{\mathsf{s}}$, by definition of $\langle X \rangle_{\mathsf{s}}$.

- By construction $P := \langle X \cup \{1\} \rangle_{\mathsf{s}}$ is a sub-semiring containing 1, in other words a sub-ring. And as $X \subseteq P$ this implies $\langle X \rangle_{\mathsf{r}} \subseteq P$. And as any sub-ring $Q \leq_{\mathsf{r}} R$ contains 1 we get $X \subseteq Q \implies X \cup \{1\} \subseteq Q \implies P \subseteq Q$. This also proves $\langle X \rangle_{\mathsf{r}} \subseteq P$, as Q has been arbitrary.

- Now suppose R is a field, and let $P := \{ ab^{-1} \mid a, b \in \langle X \rangle_{\mathsf{r}}, b \neq 0 \}$. First of all $0 = 0 \cdot 1^{-1}$ and $1 = 1 \cdot 1^{-1} \in P$. And if ab^{-1} and $cd^{-1} \in P$, then we get $(ab^{-1} + cd^{-1} = (ad + bc)(bd)^{-1} \in P$

and $(ab^{-1})(cd^{-1}) = (ab)(cd)^{-1} \in P$. And if $ab^{-1} \neq 0$ then we in particular have $a \neq 0$ and hence $(ab^{-1})^{-1} = ba^{-1} \in P$. Clearly $X \subseteq P$, as even $X \subseteq \langle X \rangle_{\mathfrak{r}}$. Altogether P is a field containing X and hence $\langle X \rangle_{\mathfrak{f}} \subseteq P$. And if conversely $Q \subseteq R$ is a field containing X, then $\langle X \rangle_{\mathfrak{r}} \subseteq Q$. Thus is $a, b \in Q$ with $b \neq 0$ then $b^{-1} \in Q$ and hence $ab^{-1} \in Q$, as Q is a field. But this proves $P \subseteq Q$ and thus $P \subseteq \langle X \rangle_{\mathfrak{f}}$.

□

Proof of (1.56):

We first have to prove, that $\mathfrak{a} \cap \mathfrak{b}$, $\mathfrak{a} + \mathfrak{b}$ and $\mathfrak{a}\,\mathfrak{b}$ truly are ideals of R. In the case of $\mathfrak{a} \cap \mathfrak{b}$ this has already been done in (1.52). For $\mathfrak{a} + \mathfrak{b}$ it is clear that $0 = 0 + 0 \in \mathfrak{a} + \mathfrak{b}$. and if $a + b$ and $a' + b' \in \mathfrak{a} + \mathfrak{b}$ then also $(a + b) + (a' + b') = (a + a') + (b + b') \in \mathfrak{a} + \mathfrak{b}$ and $-(a + b) = (-a) + (-b) \in \mathfrak{a} + \mathfrak{b}$. Thus consider any $f \in R$, as $\mathfrak{a}$ and $\mathfrak{b}$ are ideals we have fa, $af \in \mathfrak{a}$ and fb, $bf \in \mathfrak{b}$ again. Hence we get $f(a + b) = (fa) + (fb)$ and $(a + b)f = (af) + (bf) \in \mathfrak{a} + \mathfrak{b}$. Likewise $0 = 0 \cdot 0 \in \mathfrak{a}\,\mathfrak{b}$. And if $f = \sum_i a_i b_i$ and $g = \sum_j c_j d_j \in \mathfrak{a}\,\mathfrak{b}$ then it is clear from the definition that $f + g \in \mathfrak{a}\,\mathfrak{b}$. Further $-f = \sum_i (-a_i) b_i \in \mathfrak{a}\,\mathfrak{b}$ and for any arbitrary $h \in R$ we also get $hf = \sum_i (ha_i) b_i$ and $fh = \sum_i a_i (b_i h) \in \mathfrak{a}\,\mathfrak{b}$ by the same reasoning as for $\mathfrak{a} + \mathfrak{b}$.

Thus it remains to prove the chain of inclusions $\mathfrak{a}\,\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a} \subseteq \mathfrak{a} + \mathfrak{b}$. Hereby $\mathfrak{a} \subseteq \mathfrak{a} + \mathfrak{b}$ is clear by taking $b = 0$ in $a + b \in \mathfrak{a} + \mathfrak{b}$. And $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a}$ is true trivially. Thus it only remains to verify $\mathfrak{a}\,\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$. That is we consider $f = \sum_i a_i b_i \in \mathfrak{a}\,\mathfrak{b}$. Since $a_i \in \mathfrak{a}$ and $\mathfrak{a}$ is an ideal we have $a_i b_i \in \mathfrak{a}$ and hence even $f \in \mathfrak{a}$. Likewise we can verify $f \in \mathfrak{b}$ such that $f \in \mathfrak{a} \cap \mathfrak{b}$ as claimed. □

Proof of (1.57):

The associativity of $\cap$ is clear (from the associativity of the locical *and*). The associativity of ideals $(\mathfrak{a} + \mathfrak{b}) + \mathfrak{c} = \mathfrak{a} + (\mathfrak{b} + \mathfrak{c})$ is immediate from the associativity of elements $(a + b) + c = a + (b + c)$. The same is true for the commutativity of $\cap$ and $+$. Next we prove $(\mathfrak{a}\,\mathfrak{b})\,\mathfrak{c} \subseteq \mathfrak{a}\,(\mathfrak{b}\,\mathfrak{c})$. That is we are given an element of $(\mathfrak{a}\,\mathfrak{b})\,\mathfrak{c}$ which is of the form

$$\sum_{j=1}^{n} \left(\sum_{i=1}^{m} a_{i,j} b_{i,j} \right) c_j \;=\; \sum_{i=1}^{m} \sum_{j=1}^{n} a_{i,j} (b_{i,j} c_j)$$

For some $a_{i,j} \in \mathfrak{a}$, $b_{i,j} \in \mathfrak{b}$ and $c_j \in \mathfrak{c}$. However from the latter representation it is clear that this element is also contained in $\mathfrak{a}\,(\mathfrak{b}\,\mathfrak{c})$, which establishes the inclusion. The converse inclusion can be shown in complete analogy, which proves the associativity $(\mathfrak{a}\,\mathfrak{b})\,\mathfrak{c} = \mathfrak{a}\,(\mathfrak{b}\,\mathfrak{c})$. And if R is commutative the commutativity of ideals $\mathfrak{a}\,\mathfrak{b} = \mathfrak{b}\,\mathfrak{a}$ is immediate from the commuativity of the elements $ab = ba$. Thus it remains to check the distributivity

$$\mathfrak{a}\,(\mathfrak{b} + \mathfrak{c}) \;=\; (\mathfrak{a}\,\mathfrak{b}) + (\mathfrak{a}\,\mathfrak{c})$$

For the inclusion " $\supseteq$ " we are given elements $a_i \in \mathfrak{a}$, $b_i \in \mathfrak{b}$ and $c_i \in \mathfrak{c}$ (where $i \in 1 \ldots m$) such that $\sum_i a_i (b_i + c_i) \in \mathfrak{a}\,(\mathfrak{b} + \mathfrak{c})$. But it is already obvious that $\sum_i a_i (b_i + c_i) = \sum_i a_i b_i + \sum_i a_i c_i \in (\mathfrak{a}\,\mathfrak{b}) + (\mathfrak{a}\,\mathfrak{c})$. And for the converse inclusion "$\subseteq$" we are given a_i, $a'_j \in \mathfrak{a}$, $b_i \in \mathfrak{b}$ and $c_j \in \mathfrak{c}$ such that $\sum_i a_i b_i + \sum_j a'_j c_j \in (\mathfrak{a}\,\mathfrak{b}) + (\mathfrak{a}\,\mathfrak{c})$. This however can be rewritten into the form $\sum_i a_i b_i + \sum_j a'_j c_j = \sum_i a_i (b_i + 0) + \sum_j a'_j (0 + c_j) \in \mathfrak{a}\,(\mathfrak{b} + \mathfrak{c})$. In complete analogy it can be shown, that $(\mathfrak{a} + \mathfrak{b})\,\mathfrak{c} = (\mathfrak{a}\,\mathfrak{c}) + (\mathfrak{b}\,\mathfrak{c})$. □

Proof of (1.59):

By assumption we have $\mathfrak{a} = \langle X \rangle_{\mathfrak{i}}$ and $\mathfrak{b} = \langle Y \rangle_{\mathfrak{i}}$, in particular $X \subseteq \mathfrak{a}$ and $Y \subseteq \mathfrak{b}$. Hence we get

$X \cup Y \subseteq \mathfrak{a} \cup \mathfrak{b} \subseteq \mathfrak{a} + \mathfrak{b}$ and therefore $\langle X \cup Y \rangle_{\mathfrak{i}} \subseteq \mathfrak{a} + \mathfrak{b}$ (as $\mathfrak{a} + \mathfrak{b}$ is an ideal of R). For the converse inclusion we regard $f = \sum_i a_i x_i b_i \in \mathfrak{a}$ and $g = \sum_j c_j y_j d_j$ (note that this representation with $x_i \in X$ and $y_j \in Y$ is allowed, due to (1.55)). And hence we get $f + g = \sum_i a_i x_i b_i + \sum_j c_j y_j d_j \in \langle X \cup Y \rangle_{\mathfrak{i}}$. Together we have found $\mathfrak{a} + \mathfrak{b} = \langle X \cup Y \rangle_{\mathfrak{i}}$. For $\mathfrak{a}\,\mathfrak{b} = \langle X\,Y \rangle_{\mathfrak{i}}$ we have assumed R to be commutative. The one incluion is clear: as $X \subseteq \mathfrak{a}$ and $Y \subseteq \mathfrak{b}$ we trivially have $X\,Y \subseteq \mathfrak{a}\,\mathfrak{b}$. And as $\mathfrak{a}\,\mathfrak{b}$ is an ideal of R this implies $\langle X\,Y \rangle_{\mathfrak{i}} \subseteq \mathfrak{a}\,\mathfrak{b}$. For the converse inclusion we regard $f \in \mathfrak{a}$ and $g \in \mathfrak{b}$ as above. Then $fg = \sum_i \sum_j a_i b_i x_i y_j c_j d_j \in \langle X\,Y \rangle_{\mathfrak{i}}$ (due to the commutativity of R) which also establishes $\langle X\,Y \rangle_{\mathfrak{i}} = \mathfrak{a}\,\mathfrak{b}$. □

Proof of (1.60):

(i) First of all it is clear that $\mathfrak{b} \setminus \mathfrak{a} \subseteq \mathfrak{b}$. And hence we find $\langle \mathfrak{b} \setminus \mathfrak{a} \rangle_{\mathfrak{i}} \subseteq \langle \mathfrak{b} \rangle_{\mathfrak{i}} = \mathfrak{b}$ (as $\mathfrak{b}$ is an ideal already). Thus we have proved

$$\langle \mathfrak{b} \setminus \mathfrak{a} \rangle_{\mathfrak{i}} \quad \subseteq \quad \mathfrak{b}$$

Now fix any $b \in \mathfrak{b} \setminus \mathfrak{a}$ (this is possible by assumption $\mathfrak{a} \subset \mathfrak{b}$) and consider any $a \in \mathfrak{a}$. Then $a - b \in \mathfrak{b}$ but $a - b \notin \mathfrak{a}$ (else let $\alpha := a - b \in \mathfrak{a}$, then $b = a - \alpha \in \mathfrak{a}$, a contradiction). Thus $a - b \in \mathfrak{b} \setminus \mathfrak{a}$ and hence $a = b + (a - b) \in \langle \mathfrak{b} \setminus \mathfrak{a} \rangle_{\mathfrak{i}}$. As a has been arbitrary this yields $\mathfrak{a} \subseteq \langle \mathfrak{b} \setminus \mathfrak{a} \rangle_{\mathfrak{i}}$ and thereby we have also proved the converse inclusion

$$\mathfrak{b} \;=\; \mathfrak{a} \cup (\mathfrak{b} \setminus \mathfrak{a}) \;\subseteq\; \mathfrak{a} \cup \langle \mathfrak{b} \setminus \mathfrak{a} \rangle_{\mathfrak{i}} \;=\; \langle \mathfrak{b} \setminus \mathfrak{a} \rangle_{\mathfrak{i}}$$

(ii) By (1.55) the ideal generated by the union of the $\mathfrak{a}_i$ consists of finite sums of elements of the form $a_i x_i b_i$ where $a_i, b_i \in R$ and $x_i \in \mathfrak{a}_i$. But as $\mathfrak{a}_i$ is an ideal we get $a_i x_i b_i \in \mathfrak{a}_i$ already. And conversely any finite sum of elements $x_i \in \mathfrak{a}_i$ can be realized, by taking $a_i = b_i = 1$.

(iii) Here we just rewrote the the equality in (ii) in several ways: given a sum $\sum_{i \in I} a_i$ where $a_i \in \mathfrak{a}_i$ and $\Omega := \{\, i \in I \mid a_i \neq 0 \,\}$ is finite then $\sum_{i \in I} a_i = \sum_{i \in \Omega} a_i$ by definition of arbitrary sums. And likewise this is just $\sum_k a_k$ where $n := \#\Omega$, $\Omega = \{\, i(1), \ldots, i(n) \,\}$ and $a_k = a_{i(k)}$.

(iv) The general distributivity rule can be seen by a straightforward computation using the general rules of distributivity and associativity. First note that by definition and (iii) we have

$$\sum_{i \in I} \mathfrak{a}_i\,\mathfrak{b} \;=\; \left\{ \sum_{i \in \Omega} \left(\sum_{k=1}^{n(i)} a_{i,k} b_{i,k} \right) \;\middle|\; a_{i,k} \in \mathfrak{a}_i,\; b_{i,k} \in \mathfrak{b} \right\}$$

Now let $n := \max\{\, n(i) \mid i \in \Omega \,\}$ and for any $k > n(i)$ let $a_{i,k} := 0 \in \mathfrak{a}_i$. Then we may rewrite the latter set in the form

$$\sum_{i \in I} \mathfrak{a}_i\,\mathfrak{b} \;=\; \left\{ \sum_{k=1}^{n} \sum_{i \in \Omega} a_{i,k} b_{i,k} \;\middle|\; a_{i,k} \in \mathfrak{a}_i,\; b_{i,k} \in \mathfrak{b} \right\}$$

Let us now regart the other set involved. Again we will compute what this set means explictly - and thereby we will find the same identity as the one wh have just proved

$$\left(\sum_{i \in I} \mathfrak{a}_i \right) \mathfrak{b} \;=\; \left\{ \sum_{k=1}^{n} \left(\sum_{i \in \Omega(k)} a_{i,k} \right) b_k \;\middle|\; a_{i,k} \in \mathfrak{a}_i,\; b_k \in \mathfrak{b} \right\}$$

Then (in analogy to the above) we take $\Omega := \Omega(1) \cup \cdots \cup \Omega(n)$, $a_{i,k} := 0$ for $i \notin \Omega(k)$ and

$b_{i,k} := b_k$. Then this turns into

$$\left(\sum_{i\in I}\mathfrak{a}_i\right)\mathfrak{b} \;=\; \left\{\sum_{k=1}^{n}\sum_{i\in\Omega} a_{i,k}b_{i,k} \;\middle|\; a_{i,k}\in\mathfrak{a}_i,\; b_{i,k}\in\mathfrak{b}\right\}$$

□

Proof of (1.61):

(i) (a) $\Longrightarrow$ (b): $1 \in R = \mathfrak{a}+\mathfrak{b} = \{\, a+b \mid a\in\mathfrak{a}, b\in\mathfrak{b}\,\}$ is clear. Hence there are $a'\in\mathfrak{a}$ and $b\in\mathfrak{b}$ such that $1 = a'+b$. Now let $a := -a' \in \mathfrak{a}$ then $1 = (-a)+b$ and hence $b = 1+a \in (1+\mathfrak{a})\cap\mathfrak{b}$. (b) $\Longrightarrow$ (c): let $b\in(1+\mathfrak{a})\cap\mathfrak{b}$, that is there is some $a'\in\mathfrak{a}$ such that $b = 1+a'$. Again we let $a := -a' \in \mathfrak{a}$, then $a+b = 1$. (c) $\Longrightarrow$ (a): by the same reasoning as before we find $1 = a+b \in \mathfrak{a}+\mathfrak{b}$. And as $\mathfrak{a}+\mathfrak{b}$ is an ideal of R, this implies $\mathfrak{a}+\mathfrak{b} = R$.

(ii) As $\mathfrak{a}$ and $\mathfrak{b}$ are coprime there are some $a\in\mathfrak{a}$ and $b\in\mathfrak{b}$ such that $a+b=1$ - diue to (i). Using these we compute

$$\begin{aligned}
1 \;&=\; 1^{i+j} \;=\; (a+b)^{i+j} \;=\; \sum_{h=0}^{i+j}\binom{i+j}{h}a^h b^{i+j-h}\\
&=\; \sum_{h=0}^{i}\binom{i+j}{h}a^h b^{i+j-h} + \sum_{h=i+1}^{i+j} a^h b^{i+j-h}\\
&=\; b^j\sum_{h=0}^{i}\binom{i+j}{h}a^h b^{i-h} + a^i\sum_{h=1}^{j}\binom{i+j}{i+h}a^h b^{j-h}\\
&\in\; \mathfrak{b}^j + \mathfrak{a}^i
\end{aligned}$$

(iii) We will use induction on k. The case $k=1$ is trivial and hence we found the induction at $k=2$. In this case let us first choose $a_1, a_2\in\mathfrak{a}$, $b_1\in\mathfrak{b}_1$ and $b_2\in\mathfrak{b}_2$ such that $a_1+b_1 = 1$ and $a_2+b_2 = 1$. Then

$$b_1b_2 \;=\; (1-a_1)(1-a_2) \;=\; 1-a_1-a_2+a_1a_2$$

This implies $1 = (a_1+a_2-a_1a_2)+b_1b_2 \in \mathfrak{a}+\mathfrak{b}_1\mathfrak{b}_2$ which rests the case $k=2$. So we now assume $k\geq 2$ and are given $\mathfrak{a}+\mathfrak{b}_i = R$ for any $i\in 1\ldots k+1$. By induction hypothesis we in particular get $\mathfrak{a}+\mathfrak{b}_1\ldots\mathfrak{b}_k = R$. And together with $\mathfrak{a}+\mathfrak{b}_{k+1} = R$ and the case $k=2$ this yields the induction step $\mathfrak{a}+(\mathfrak{b}_1\ldots\mathfrak{b}_k)\mathfrak{b}_{k+1} = R$.

(iv) We will prove the two inclusions by induction on k separately. The case $k=1$ is trivial, so we will start with $k=2$ only. In this case the inclusion $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}_1\cap\mathfrak{a}_2$ has already been proved. And if $k\geq 2$ then

$$(\mathfrak{a}_1\ldots\mathfrak{a}_k)\mathfrak{a}_{k+1} \;\subseteq\; (\mathfrak{a}_1\ldots\mathfrak{a}_k)\cap\mathfrak{a}_{k+1} \;\subseteq\; (\mathfrak{a}_1\cap\cdots\cap\mathfrak{a}_k)\cap\mathfrak{a}_{k+1}$$

due to the case $k=2$ and the induction hypothesis respectively. For the converse inclusion we start with $k=2$ again. And as $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are coprime we may find $a_1\in\mathfrak{a}_1$ and $a_2\in\mathfrak{a}_2$ such that $a_1+a_2 = 1$. If now $x\in\mathfrak{a}_1\cap\mathfrak{a}_2$ is an arbitrary element then

$$x \;=\; x1 \;=\; x(a_1+a_2) \;=\; xa_1+xa_2 \;=\; a_1x+a_2x \;\in\; \mathfrak{a}_1\mathfrak{a}_2$$

This proves $\mathfrak{a}_1 \cap \mathfrak{a}_2 \subseteq \mathfrak{a}_1\mathfrak{a}_2$ and hence we may commence with $k \geq 2$. In this case we are given some $x \in \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_k \cap \mathfrak{a}_{k+1}$. In particular this is $x \in \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_k$ and hence $x \in \mathfrak{a}_1 \ldots \mathfrak{a}_k$ by induction hypothesis. Thus we get $x \in (\mathfrak{a}_1 \ldots \mathfrak{a}_k) \cap \mathfrak{a}_{k+1}$. But because of (iii) (using $\mathfrak{a} := \mathfrak{a}_{k+1}$ and $\mathfrak{b}_i := \mathfrak{a}_i$) we know that $\mathfrak{a}_1 \ldots \mathfrak{a}_k$ and $\mathfrak{a}_{k+1}$ are coprime. Therefore we may apply the case $k = 2$ again to finally find $x \in (\mathfrak{a}_1 \ldots \mathfrak{a}_k)\mathfrak{a}_{k+1}$.

□

Proof of (1.62):
We first prove that $\sim$ is an equivalence relation: *Reflexivity* $a \sim a$ is clear, as $a - a = 0 \in \mathfrak{a}$. *Symmetry* if $a \sim b$ then $a - b \in \mathfrak{a}$ and hence $b - a = -(a - b) \in \mathfrak{a}$ which proves $b \sim a$. *Transitivity* if $a \sim b$ and $b \sim c$ then $a - c = (a - b) + (b - c) \in \mathfrak{a}$ such that $a \sim c$. If now $a \in R$ then

$$\begin{aligned} [a] &= \{\, b \in R \mid a \sim b \,\} = \{\, b \in R \mid a - b \in \mathfrak{a} \,\} \\ &= \{\, b \in R \mid \exists h \in \mathfrak{a} : a - b = h \,\} \\ &= \{\, a + h \mid h \in \mathfrak{a} \,\} = a + \mathfrak{a} \end{aligned}$$

Now assume that $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ even is an ideal, then we have to prove, that $R/\mathfrak{a}$ is a ring under the operations $+$ and $\cdot$ as we have introduced them. Thus we prove the well-definedness: suppose $a + \mathfrak{a} = a' + \mathfrak{a}$ and $b + \mathfrak{a} = b' + \mathfrak{a}$ then $a - a'$ and $b - b' \in \mathfrak{a}$ and hence $(a + b) - (a' + b') = (a - a') + (b - b') \in \mathfrak{a}$. This means $a + b \sim a' + b'$ and hence $(a + b) + \mathfrak{a} = (a' + b') + \mathfrak{a}$. Analogously

$$ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b')$$

As $\mathfrak{a}$ is an ideal both $(a - a')b$ and $a'(b - b')$ are contained in $\mathfrak{a}$ and hence also the sum $ab - a'b' \in \mathfrak{a}$. This means $ab \sim a'b'$ and hence $ab + \mathfrak{a} = a'b' + \mathfrak{a}$. Hence these operations are well-defined. And all the properties (associativity, commutativity, distributivity and so forth) are immediate from the respective properties of R. This also shows that $1 + \mathfrak{a}$ is the unit element of $R/\mathfrak{a}$ (supposed 1 is the unit element of R). □

Proof of (1.64):
First of all we have (a) $\implies$ (c) because $b \in b + n\mathbb{Z} = a + n\mathbb{Z}$ gives some $c \in n\mathbb{Z}$ such that $b = a + c$. And $c \in n\mathbb{Z}$ means nothing but $c = kn$ for some $k \in \mathbb{Z}$. For (c) $\implies$ (b) we use division with remainder (1.28) to write $a = pn + r$ and $b = qn + s$ such that $r = a \mod n$ and $s = b \mod n$. Then we can compute

$$qn + s = b = a + kn = pn + r + kn = (p + k)n + r$$

which yields $s - r = (p + k - q)n$ such that $|s - r| = |p + k - q| \cdot n$. As r and s both are positive, this implies that $0 \leq |s - r| < \max\{\, s, r \,\} < n$. But this can only be, if $|p + k - q| = 0$ such that $q = n + k$ and $r = s$. And the latter just is the claim (b). It remains to prove (b) $\implies$ (a): continueing with the notation we have $r = s$ and hence $b - a = qn + s - qn - r = (q - p)n$. Letting $k := q - p$ we have $b - a = kn \in n\mathbb{Z}$. That is a and b are equivalent and hence have the same equivalence classes $a + n\mathbb{Z} = b + n\mathbb{Z}$. □

Proof of (1.66):

- We first prove that $\mathfrak{b}/\mathfrak{a}$ truly is an ideal of $R/\mathfrak{a}$. Thus regard $a + \mathfrak{a}$ and $b + \mathfrak{a} \in \mathfrak{b}/\mathfrak{a}$, that is a,

$b \in \mathfrak{b}$. Then we clearly get $a+b$ and $-a \in \mathfrak{b}$ such that $(a+\mathfrak{a})+(b+\mathfrak{a}) = (a+b)+\mathfrak{a} \in \mathfrak{b}/\mathfrak{a}$ and $-(a+\mathfrak{a}) = (-a)+\mathfrak{a} \in \mathfrak{b}/\mathfrak{a}$. Further if $f+\mathfrak{a} \in R/\mathfrak{a}$ (that is $f \in R$) then fb, $bf \in \mathfrak{b}$, as $\mathfrak{b}$ is an ideal. And hence $(f+\mathfrak{a})(b+\mathfrak{a}) = (fb)+\mathfrak{a} \in \mathfrak{b}/\mathfrak{a}$, likewise $(b+\mathfrak{a})(f+\mathfrak{a}) \in \mathfrak{b}/\mathfrak{a}$.

- Next we prove that $\mathfrak{b} := \{b \in R \mid b+\mathfrak{a} \in \mathfrak{u}\} \trianglelefteq_{\mathfrak{i}} R$ is an ideal, supposed $\mathfrak{u} \trianglelefteq_{\mathfrak{i}} R/\mathfrak{a}$ is an ideal. Thus consider a, $b \in \mathfrak{b}$ then $(a+b)+\mathfrak{a} = (a+\mathfrak{a})+(b+\mathfrak{a}) \in \mathfrak{u}$ and $(-a)+\mathfrak{a} = -(a+\mathfrak{a}) \in \mathfrak{u}$ which proves $a+b$ and $-a \in \mathfrak{b}$. And if $f \in R$ then $(fb)+\mathfrak{a} = (f+\mathfrak{a})(b+\mathfrak{a}) \in \mathfrak{u}$ which proves $fb \in \mathfrak{b}$ (likewise $bf \in \mathfrak{b}$. Hence $\mathfrak{b}$ is an ideal, and $\mathfrak{a} \subseteq \mathfrak{b}$ is clear, as for any $a \in \mathfrak{a}$ we get $a+\mathfrak{a} = 0+\mathfrak{a} \in \mathfrak{u}$.

- Thus we have proved that the maps $\mathfrak{b} \mapsto \mathfrak{b}/\mathfrak{a}$ and $\mathfrak{u} \mapsto \mathfrak{b}$ are well defined. We now claim that they even are mutually inverse. For the first composition we start with $\mathfrak{a} \subseteq \mathfrak{b} \trianglelefteq_{\mathfrak{i}} R$. Then

$$\mathfrak{b} \;\mapsto\; \mathfrak{b}\Big/_{\mathfrak{a}} \;\mapsto\; \left\{ b \in R \mid b+\mathfrak{a} \in \mathfrak{b}\Big/_{\mathfrak{a}} \right\} \;=\; \{\, b \mid b \in \mathfrak{b} \,\} \;=\; \mathfrak{b}$$

 For the converse composition we start with an ideal $\mathfrak{u} \trianglelefteq_{\mathfrak{i}} R/\mathfrak{a}$, which is mapped to $\mathfrak{b} := \{b \in R \mid b+\mathfrak{a} \in \mathfrak{u}\}$. Now it is easy to see that

$$\mathfrak{u} \;\mapsto\; \mathfrak{b} \;\mapsto\; \mathfrak{b}\Big/_{\mathfrak{a}} \;=\; \{\, b+\mathfrak{a} \mid b+\mathfrak{a} \in \mathfrak{u} \,\} \;=\; \mathfrak{u}$$

(i) By now we have established the correspondence of ideals. In the next step we need to prove, that this correspondence is compatible with the generation of ideals: For the inclusion " $\supseteq$ " we begin with any $u \in \langle X/\mathfrak{a}\rangle_{\mathfrak{i}}$. That is there are $a_i+\mathfrak{a}$, $b_i+\mathfrak{a} \in R/\mathfrak{a}$ and $x_i+\mathfrak{a} \in X/\mathfrak{a}$ such that

$$\begin{aligned} u &= \sum_{i=1}^{k} (a_i+\mathfrak{a})(x_i+\mathfrak{a})(b_i+\mathfrak{a}) \\ &= \left(\sum_{i=1}^{k} a_i x_i b_i\right) + \mathfrak{a} \;\in\; \langle X\rangle_{\mathfrak{i}} + \mathfrak{a}\Big/_{\mathfrak{a}} \end{aligned}$$

 And for the converse inclusion " $\subseteq$ " we are given some $a \in \mathfrak{a}$ and $y \in \langle X\rangle_{\mathfrak{i}}$. The element y generated by X is of the follwing form: There are some a_i, $b_i \in R$ and $x_i \in X$ such that $y = \sum_i a_i x_i b_i$. Using this we undo the above computation to find

$$(a+y)+\mathfrak{a} \;=\; y+\mathfrak{a} \;=\; \sum_{i=1}^{k} (a_i+\mathfrak{a})(x_i+\mathfrak{a})(b_i+\mathfrak{a}) \;\in\; \langle X\Big/_{\mathfrak{a}}\rangle_{\mathfrak{i}}$$

(ii) The identity of the sums is a no-brainer: The elements of the sum of the ideals $\mathfrak{b}_i$ are finite sums $b_1+\cdots+b_n$ where $b_k \in \mathfrak{b}_{i(k)}$ for some $i(k) \in I$. But then we immediately find

$$\left(\sum_{k=1}^{n} b_k\right) + \mathfrak{a} \;=\; \sum_{k=1}^{n} (b_k+\mathfrak{a}) \;\in\; \sum_{k=1}^{n} \mathfrak{b}_{i(k)}\Big/_{\mathfrak{a}} \;\subseteq\; \sum_{i\in I} \mathfrak{b}_i\Big/_{\mathfrak{a}}$$

 Conversely the elements of the sum of quotient ideals $\mathfrak{b}_i/\mathfrak{a}$ are finite sums of the following form,

where $b_k \in \mathfrak{b}_{i(k)}$ for some $i(k) \in I$ again. Thus the same computation reversed yields

$$\sum_{k=1}^{n} (b_k + \mathfrak{a}) \;=\; \left(\sum_{k=1}^{n} b_k \right) + \mathfrak{a} \;\in\; \textstyle\sum_{k=1}^{n} \mathfrak{b}_{i(k)} \Big/ \mathfrak{a} \;\subseteq\; \sum_{i \in I} \mathfrak{b}_i \Big/ \mathfrak{a}$$

(ii) Now to the identity of the intersections, the inclusion " $\supseteq$ " is elementary logic: If we regard any $x + \mathfrak{a}$, where x is contained in the intersection of the $\mathfrak{b}_i$ then $x \in \mathfrak{b}_i$ for any $i \in I$. Hence $x + \mathfrak{a} \in \mathfrak{b}_i/\mathfrak{a}$ is granted. And as this is true for any $i \in I$ we find $x + \mathfrak{a}$ in the intersection of the $\mathfrak{b}_i/\mathfrak{a}$. The converse inclusion "$\subseteq$" makes use of the ideals: Consider any $x + \mathfrak{a}$ in the intersection of the $\mathfrak{b}_i/\mathfrak{a}$. That is for any $i \in I$ there is some $b_i \in \mathfrak{b}_i$ such that $x + \mathfrak{a} = b_i + \mathfrak{a}$. But we need the same b for all $i \in I$. So fix any $j \in I$, let $b := b_j$ and consider any $i \in I$. As $b + \mathfrak{b}_j = x + \mathfrak{a} = b_i + \mathfrak{a}$ we get $a_i := b - b_i \in \mathfrak{a}$. But we clearly have $b = b_i + a_i$ and $b_i \in \mathfrak{b}_i$ and $a_i \in \mathfrak{a} \subseteq \mathfrak{b}_i$ by construction. Thus we see, that $b \in \mathfrak{b}_i$ and as $i \in I$ was arbitrary, this means $b \in \bigcap_i \mathfrak{b}_i$. And from this we get

$$x + \mathfrak{a} \;=\; b + \mathfrak{a} \;\in\; \bigcap_{i \in I} \mathfrak{b}_i \Big/ \mathfrak{a}$$

(iii) Now for the identity of the product of finitely many ideals: Let us use induction on the number $n := \#I$ of ideals involved. For $n = 1$ the statement is trivial. For the induction step we may regard $\mathfrak{b} := \mathfrak{b}_1 \ldots \mathfrak{b}_n$ and $\mathfrak{c} := \mathfrak{b}_{n+1}$ as the multiplication of ideals is associative. So it suffices to regard the case $n = 2$, that is two ideals $\mathfrak{b}$ and $\mathfrak{c} \trianglelefteq_{\mathrm{i}} R$ with $\mathfrak{a} \subseteq \mathfrak{b}$ and $\mathfrak{a} \subseteq \mathfrak{c}$. For these we find the identity

$$\begin{aligned} \mathfrak{b} \Big/ \mathfrak{c} \,\Big/ \mathfrak{c} \;&=\; \left\{ \sum_{i=1}^{n} (b_i + \mathfrak{a})(c_i + \mathfrak{a}) \;\middle|\; b_i \in \mathfrak{b}, c_i \in \mathfrak{c} \right\} \\ &=\; \left\{ \left(\sum_{i=1}^{n} b_i c_i \right) + \mathfrak{a} \;\middle|\; b_i \in \mathfrak{b}, c_i \in \mathfrak{c} \right\} \;=\; \mathfrak{b}\,\mathfrak{c} \Big/ \mathfrak{c} \end{aligned}$$

- We now prove that this correspondence even interlocks radical ideals. First note that $\mathfrak{b} \trianglelefteq_{\mathrm{i}} R$ is radical iff $\sqrt{\mathfrak{b}} = \mathfrak{b}$. Now remark that $(b + \mathfrak{a})^k = b^k + \mathfrak{a} \in \mathfrak{b}/\mathfrak{a}$ is (by definition) equivalent to $b^k \in \mathfrak{b}$. Thus we found

 $$\sqrt{\mathfrak{b} \Big/ \mathfrak{a}} \;=\; \sqrt{\mathfrak{b}} \Big/ \mathfrak{a}$$

 And in particular we see that $\mathfrak{b}/\mathfrak{a}$ is a redical ideal if and only if $\mathfrak{b}$ is a radical ideal. And this has been claimed.

- If $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R/\mathfrak{a}$ is prime then regard any $a, b \in R$. Then $(a + \mathfrak{a})(b + \mathfrak{a}) = ab + \mathfrak{a} \in \mathfrak{p}/\mathfrak{a}$ is equivalent, to $ab \in \mathfrak{p}$ which again is equivalent, to $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$ (as $\mathfrak{p}$ is prime). And again this is equivalent, to $a + \mathfrak{a} \in \mathfrak{p}/\mathfrak{a}$ or $b + \mathfrak{a} \in \mathfrak{p}/\mathfrak{a}$. Hence $\mathfrak{p}/\mathfrak{a}$ is prime, too. For the converse implication just pursue the same arguments in inverse order.

- As the correspondence $\mathfrak{b} \longleftrightarrow \mathfrak{b}/\mathfrak{a}$ maintains the inclusion $\subseteq$ of subsets, it is clear that maximal elements mutually correspond to each other. That is $\mathfrak{m}/\mathfrak{a}$ is maximal, if and only if $\mathfrak{m}/\mathfrak{a}$ is maximal.

□

Proof of (1.76):

(i) Clearly $\varphi(0_R) = \varphi(0_R + 0_R) = \varphi(0_R) + \varphi(0_R)$ and subtracting $\varphi(0_R)$ from this equation (i.e. adding $-\varphi(0_R)$ to both sides of the equation) we find $0_S = \varphi(0_R)$. Hence $\varphi(a) + \varphi(-a) = \varphi(a - a) = \varphi(0_R) = 0_S$ which proves that $\varphi(-a)$ is the negative $-\varphi(a)$.

(ii) Analogous to the above we find $1_S = \varphi(1_R) = \varphi(uu^{-1}) = \varphi(u)\varphi(u^{-1})$ and $1_S = \varphi(1_R) = \varphi(u^{-1}u) = \varphi(u^{-1})\varphi(u)$ which proves that $\varphi(u^{-1})$ is the inverse $\varphi(u)^{-1}$.

(iii) If $a, b \in R$ then $\psi\varphi(a+b) = \psi(\varphi(a) + \psi(b)) = \psi\varphi(a) + \psi\varphi(b)$ and likewise for the multiplication. Hence $\psi\varphi$ is a homomorphism of semi-rings again. And in the case of rings and homomorphisms of rings we also get $\psi\varphi(1_R) = \psi(1_S) = 1_T$.

(iv) Consider any $x, y \in S$, as Φ is surjective there are $a, b \in R$ such that $x = \Phi(a)$ and $y = \Phi(b)$. Now $\Phi^{-1}(x+y) = \Phi^{-1}(\Phi(a) + \Phi(b)) = \Phi^{-1}\Phi(a+b) = a + b = \Phi^{-1}(x) + \Phi^{-1}(y)$. Likewise we find $\Phi^{-1}(xy) = \Phi^{-1}(x)\Phi^{-1}(y)$. And if Φ is a homomorphism of rings, then $\Phi^{-1}(1_S) = 1_R$ is clear from $\Phi(1_R) = 1_S$.

(v) Since $\mathrm{im}(\varphi) = \varphi(R)$ the first statement is clear from (vi) by taking $P = R$. So we only have to prove, that $\mathrm{kn}(\varphi)$ is an ideal of R. First of all we have $0_R \in \mathrm{kn}(\varphi)$ since $\varphi(0_R) = 0_S$ by (i). And if $a, b \in \mathrm{kn}(\varphi)$ then $\varphi(a+b) = \varphi(a) + \varphi(b) = 0_S + 0_S = 0_S$ and hence $a + b \in \mathrm{kn}(\varphi)$. Analogously $\varphi(-a) = -\varphi(a) = -0_S = 0_S$ yields $-a \in \mathrm{kn}(\varphi)$. Now let $a \in \mathrm{kn}(\varphi)$ again and let $b \in R$ be arbitrary. Then $\varphi(ab) = \varphi(a)\varphi(b) = 0_S\varphi(b) = 0_S$ and hence $ab \in \mathrm{kn}(\varphi)$ again. Likewise $\varphi(ba) = \varphi(b)\varphi(a) = \varphi(b)0_S = 0_S$ which yields $ba \in \mathrm{kn}(\varphi)$.

(vi) As P is a sub-semi-ring of R we have $0_R \in P$ and therefore $0_S = \varphi(0_R) \in \varphi(P)$. Now assume that $x = \varphi(a)$ and $y = \varphi(b) \in \varphi(P)$ for some $a, b \in P$. As P is a sub-semi-ring of R we have $a + b$, $-a$ and $ab \in P$ again. And hence $x + y = \varphi(a) + \varphi(b) = \varphi(a+b) \in \varphi(P)$, $-x = -\varphi(a) = \varphi(-a) \in \varphi(P)$ and $xy = \varphi(a)\varphi(b) = \varphi(ab) \in \varphi(P)$. Thus we have proved that $\varphi(P) \leq_{\mathrm{s}} R$ is a sub-semi-ring again. And if R and S even are rings, P is a sub-ring of R and φ is a homomorphism of rings, then also $1_S = \varphi(1_R) \in \varphi(P)$ as $1_R \in P$.

(vi) And as Q is a sub-semi-ring of S we have $0_S \in Q$ and therefore $0_S = \varphi(0_R)$ implies $0_R \in \varphi^{-1}(Q)$. Now suppose $a, b \in \varphi^{-1}(Q)$, that is $\varphi(a), \varphi(b) \in Q$. Then $\varphi(a+b) = \varphi(a) + \varphi(b)$, $\varphi(-a) = -\varphi(a)$ and $\varphi(ab) = \varphi(a)\varphi(b) \in Q$, as $Q \leq_{\mathrm{s}} S$. This means that $a + b$, $-a$ and $ab \in \varphi^{-1}(Q)$ and hence $\varphi^{-1}(Q) \leq_{\mathrm{s}} S$ is a sub-semi-ring of S. And in the case of rings we also find $1_R \in \varphi^{-1}(Q)$ as in (vi) above.

(vii) First assume that $\mathfrak{b} \leq_{\mathrm{m}} S$ is a left-ideal of S. We have already proved in (vi) that $\varphi^{-1}(\mathfrak{b}) \leq_{\mathrm{s}} S$ is a sub-semi-ring of S (since $Q := \mathfrak{b} \leq_{\mathrm{s}} R$). Thus it only remains to verify the following: consider any $a \in R$ and $b \in \varphi^{-1}(\mathfrak{b})$. Then $\varphi(b) \in \mathfrak{b}$ and as $\mathfrak{b} \leq_{\mathrm{m}} S$ we hence get $\varphi(ab) = \varphi(a)\varphi(b) \in \mathfrak{b}$. Thus $ab \in \varphi^{-1}(\mathfrak{b})$ which means that $\varphi^{-1}(\mathfrak{b})$ is a left-ideal of R again. And in the case that $\mathfrak{b} \trianglelefteq_{\mathrm{i}} S$ even is an ideal, then by the same reasoning $\varphi(ba) = \varphi(b)\varphi(a) \in \mathfrak{b}$ and hence $ba \in \varphi^{-1}(\mathfrak{b})$.

(vii) Next assume that $\mathfrak{a} \leq_{\mathrm{m}} R$ is a left-ideal of R and that φ is surjective. Then $\varphi(\mathfrak{a}) \leq_{\mathrm{s}} S$ is a sub-semi-ring of S by (vi) for $P := \mathfrak{a} \leq_{\mathrm{s}} R$. Thus it again remains to prove the following property: Consider any $y \in S$ and $x = \varphi(a) \in \varphi(\mathfrak{a})$ (where $a \in \mathfrak{a}$). As φ is surjective there is some $b \in R$ with $y = \varphi(b)$. And as $ba \in \mathfrak{a}$ we hence find $yx = \varphi(b)\varphi(a) = \varphi(ba) \in \varphi(\mathfrak{a})$. Thus $\varphi(\mathfrak{a}) \leq_{\mathrm{m}} S$

is a left ideal of S. And in the case that $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ even is an ideal, then by the same reasoning $xy = \varphi(a)\varphi(b) = \varphi(ab) \in \varphi(\mathfrak{a})$.

(viii) Let $\varphi : R \to S$ be a homomorphism of semi-rings. If $\varphi(1_R) = 0_S$ then for any $a \in R$ we get $\varphi(a) = \varphi(1_R a) = 0_S \varphi(a) = 0_S$ and hence $\varphi = 0$. Else we have $\varphi(1_R) = \varphi(1_R 1_R) = \varphi(1_R)\varphi(1_R)$ and dividing by $0 \neq \varphi(1_R)$ (i.e. multiplying by $\varphi(1_R)^{-1}$) we hence find $1_S = \varphi(1_R)$.

(ix) As we have seen in (v) $\mathrm{kn}(\varphi) \trianglelefteq_{\mathrm{i}} R$ is an ideal of R. And as R is a skew-field, it has precisely two ideals: $\{0\}$ and R. In the first case $\mathrm{kn}(\varphi) = R$ we trivially have $\varphi = 0$. And in the second case $\mathrm{kn}(\varphi) = \{0\}$ we will soon see, that φ is injective.

□

Proof of (1.77):
If $b \in \mathfrak{b} \subseteq \mathfrak{a} + \mathfrak{b}$ then $\varrho(b) = b + \mathfrak{a} \in (\mathfrak{a} + \mathfrak{b})/\mathfrak{a}$ is clear and hence $\varrho(\mathfrak{b}) \subseteq (\mathfrak{a} + \mathfrak{b})/\mathfrak{a}$. Conversely for any $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ we get $(a + b) + \mathfrak{a} = b + \mathfrak{a} = \varrho(b)$ and hence $(\mathfrak{a} + \mathfrak{b})/\mathfrak{a} \subseteq \varrho(\mathfrak{b})$ as well.
Now consider any $r \in \varrho^{-1}(\varrho(\mathfrak{b}))$ that is $\varrho(r) \in \varrho(\mathfrak{b})$. That is there is some $b \in \mathfrak{b}$ such that $r + \mathfrak{a} = \varrho(r) = \varrho(b) = b + \mathfrak{a}$. That is $r - b \in \mathfrak{a}$ and hence $r - b = a$ for some $a \in \mathfrak{a}$. In other words $r = a + b \in \mathfrak{a} + \mathfrak{b}$ which proves $\varrho^{-1}(\varrho(\mathfrak{b})) \subseteq \mathfrak{a} + \mathfrak{b}$. Conversely consider any $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$. Then $\varrho(a + b) = a + b + \mathfrak{a} = b + \mathfrak{a} = \varrho(b) \in \varrho(\mathfrak{b})$ and hence $a + b \in \varrho^{-1}(\varrho(\mathfrak{b}))$. □

Proof of (1.80):

(i) By definition φ is surjective iff any $x \in S$ can be reached as $x = \varphi(a)$ for some $a \in R$. And this is just $S \subseteq \varphi(R) = \mathrm{im}(\varphi)$, or equivalently $S = \mathrm{im}(\varphi)$. And if φ is injective then there can be at most one $a \in R$ such that $\varphi(a) = 0_S$. And as $\varphi(0_R) = 0_S$ this implies $\mathrm{kn}(\varphi) = \{\, 0_R \,\}$. Conversely suppose $\mathrm{kn}(\varphi) = \{\, 0_R \,\}$ and consider $a, b \in R$ with $\varphi(a) = \varphi(b)$. Then $0_S = \varphi(a) - \varphi(b) = \varphi(a - b)$. Hence $a - b \in \mathrm{kn}(\varphi)$ such that $a - b = 0_R$ by assumption. Hence φ is injective.

(ii) The implication (a) $\implies$ (b) is clear: Just let $\Psi := \Phi^{-1}$ then we have already seen in (1.76.(iv)), that Ψ is a homomorphism of (semi-)rings again. And the converse (b) $\implies$ (a) is clear (in particular Ψ is an inverse mapping of Φ). The implication (b) $\implies$ (c) is trivial - just let $\alpha := \Psi$ and $\beta := \Psi$. And for the converse (c) $\implies$ (a) we simply compute: $\alpha = \alpha \mathbb{1}_S = \alpha(\Phi\beta) = (\alpha\Phi)\beta = \mathbb{1}_R\beta = \beta$. Thus letting $\Psi := \alpha = \beta$ we have $\Psi = \Phi^{-1}$, such that Φ is bijective.

(iii) Suppose R is a ring, then let $f := \Phi(1_R)$. If now $x \in S$ is any element then we choose $a \in R$ such that $x = \Phi(a)$. And thereby we get $fx = \Phi(1_R)\Phi(a) = \Phi(1_R a) = \Phi(a) = x$ and likewise $xf = x$. Hence $f = 1_S$ is the unit element of S and hence S is a ring, too. Further we have seen $\Phi(1_R) = 1_S$ such that Φ is a homomorphism of rings.

Suppose S is a ring, then let $e := \Phi^{-1}(1_S)$. If now $a \in R$ is any element, then $\Phi(a) = \Phi(a)1_S = \Phi(a)\Phi(e) = \Phi(ae)$ and hence $a = ae$. Likewise we see $ea = a$ and hence $e = 1_R$ is the unit element of R. Hence R is a ring, too and $\Phi(1_R) = 1_S$ is a homomorphism of rings.

(iv) Clearly the identity map $\mathbb{1}_R : R \to R : a \mapsto a$ is both, bijective and a homomorphism of (semi-)rings for any (semi-)ring $(R, +, \cdot)$. But this is nothing but the claim $\mathbb{1}_R : R \cong_{\mathrm{r}} R$. And if $\Phi : R \to S$ is an isomorphism of (semi-)rings, then Φ^{-1} is a bijective (this is clear) homomorphism of (semi-)rings again (this has already been proved). Hence the second implication. And if both $\Phi : R \cong_{\mathrm{r}} S$ and

$\Psi : S \cong_r T$ then $\Psi\Phi$ is bijective and a homomorphism of (semi-)rings (as Φ and Ψ are such). And this has been the third implication.

□

Proof of (1.83):

(i) We first need to check, that $\widetilde{\varphi}$ is well-defined: thus consider $b, c \in R$ such that $b + \mathfrak{a} = c + \mathfrak{a}$. That is $c - b \in \mathfrak{a} \subseteq \mathrm{kn}\varphi$. And hence $0 = \varphi(c-b) = \varphi(c) - \varphi(b)$ which is the well-definedness $\varphi(b) = \varphi(c)$. Now it is straightforward to see, that $\widetilde{\varphi}$ also is a homomorphism

$$\begin{aligned}
\widetilde{\varphi}\Big((b+\mathfrak{a})+(c+\mathfrak{a})\Big) &= \widetilde{\varphi}\Big((b+c)+\mathfrak{a}\Big) = \varphi(b+c) \\
&= \varphi(b)+\varphi(c) = \widetilde{\varphi}(b+\mathfrak{a})+\widetilde{\varphi}(b+\mathfrak{a}) \\
\widetilde{\varphi}\Big((b+\mathfrak{a})(c+\mathfrak{a})\Big) &= \widetilde{\varphi}\Big((bc)+\mathfrak{a}\Big) = \varphi(bc) \\
&= \varphi(b)\varphi(c) = \widetilde{\varphi}(b+\mathfrak{a})\widetilde{\varphi}(b+\mathfrak{a})
\end{aligned}$$

Thus $\widetilde{\varphi}$ always is a homomorphism of semi-rings. And if if R and S even are rings, then $R/\mathfrak{a}$ is a ring as well with the unit element $1 + \mathfrak{a}$. Thus if $\varphi(1) = 1$ is a ring-homomorphism, then $\widetilde{\varphi}(1+\mathfrak{a}) = \varphi(1) = 1$ is a ring-homomorphism, too.

(ii) Let $\mathfrak{a} := \mathrm{kn}(\varphi)$ and $\Phi := \widetilde{\varphi}$, then by (i) Φ is a well-defined (semi-)ring-homomorphism and the image of Φ certainly is the image of φ

$$\mathrm{im}(\Phi) = \Phi\left(R\big/_{\mathfrak{a}}\right) = \varphi(R) = \mathrm{im}(\varphi)$$

Hence the mapping $\Phi : R/\mathfrak{a} \to \mathrm{im}(\varphi)$ is surjective by definition. But it also is injectitve (and hence an isomorphism) due, to

$$\begin{aligned}
\varphi(a) = \varphi(b) &\iff 0 = \varphi(a) - \varphi(b) = \varphi(a-b) \\
&\iff a - b \in \mathrm{kn}(\varphi) \\
&\iff a + \mathrm{kn}(\varphi) = b + \mathrm{kn}(\varphi)
\end{aligned}$$

(iii) We will first prove that $\mathfrak{b} + R \leq_r S$ is a sub-ring of S: clearly we have $0 = 0 + 0 \in \mathfrak{b} + R$ and (if R is a sub-ring of S) $1 = 0 + 1 \in \mathfrak{b} + R$. Now let $b + a$ and $d + c \in \mathfrak{b} + R$, then

$$\begin{aligned}
(b+a)+(d+a) &= (b+d)+(a+c) \in \mathfrak{b}+R \\
-(b+a) &= (-b)+(-a) \in \mathfrak{b}+R \\
(b+a)(d+c) &= (bd+bc+ad)+ac \in \mathfrak{b}+R
\end{aligned}$$

And hence $\mathfrak{b} + R$ is a sub-ring of S. And as $\mathfrak{b} \trianglelefteq_i R$ is an ideal of S with $\mathfrak{b} \subseteq \mathfrak{b} + R$ it trivially also is an ideal $\mathfrak{b} \trianglelefteq_i \mathfrak{b} + R$. Now let us denote the restriction of the canonical epimorphism $\sigma : S \to S/\mathfrak{b}$ to R by

$$\varrho : R \to S\big/_{\mathfrak{b}} : a \mapsto a + \mathfrak{b}$$

Then ϱ is a homomorphism with kernel $\mathrm{kn}(\varrho) = \mathrm{kn}(\sigma) \cap R = \mathfrak{b} \cap R$. In particular this proves that $\mathfrak{b} \cap R \trianglelefteq_i R$ is an ideal of R (as it is the kernel of a homomorphism). And it is straightforward to

see, that $\mathrm{im}(\varphi) = (\mathfrak{b}+R)/\mathfrak{b}$. [For any $a \in R$ we have $a \in \mathfrak{b}+R$ and hence $\varrho(a) \in (\mathfrak{b}+R)/\mathfrak{b}$. And if conversely $x = b+a \in \mathfrak{b}+R$ then $\varrho(a) = a+\mathfrak{b} = x+\mathfrak{b}$]. Thus we may apply the first isomorphism theorem (ii) to obtain

$$\begin{array}{rcccl} R\big/_{\mathrm{kn}(\varrho)} & = & R\big/_{\mathfrak{b}\cap R} & \cong_{\mathsf{r}} & \mathrm{im}(\varrho) \;=\; \mathfrak{b}+R\big/_{\mathfrak{b}} \\ & & a+\mathfrak{b}\cap R & \mapsto & \varrho(a) \;=\; a+\mathfrak{b} \end{array}$$

(iv) Suppose c and $d \in R$ with $c+\mathfrak{a} = d+\mathfrak{a}$. Then $c-d \in \mathfrak{a} \subseteq \mathfrak{b}$ and hence $c+\mathfrak{b} = d+\mathfrak{b}$. Therfore we may define the following mapping (which clearly is a homomorphism of (semi-)rings)

$$\varphi \;:\; R\big/_{\mathfrak{a}} \to R\big/_{\mathfrak{b}} \;:\; c+\mathfrak{a} \mapsto c+\mathfrak{b}$$

And clearly $\mathrm{kn}(\varphi) = \{\, b+\mathfrak{a} \mid b+\mathfrak{b} = 0+\mathfrak{b} \,\} = \{\, b+\mathfrak{a} \mid b \in \mathfrak{b} \,\} = \mathfrak{b}/\mathfrak{a}$. Hence we immediately obtain (iv) from the first isomorphism theorem.

□

Proof of (1.85):

(i) Let C denote the intersection $C = \{\, a \in R \mid \forall\, i \in I \;:\; a \in C_i \,\}$, then it is clear that $0,\, 1 \in C$, as any C_i is a positive cone and hence $0,\, 1 \in C_i$. Likewise, if $a,\, b \in C$ then for any $i \in I$ we have $a,\, b \in C_i$ and hence $a+b \in C_i$ and $a \cdot b \in C_i$, as C_i was supposed to be a positive cone. Yet this again means $a+b \in C$ and $a \cdot b \in C$, such that C is a positive cone again.

(ii) It remains to show, that $\mathrm{cone}(A)$ is well-defined. However, as R itself is a positive cone and $C \subseteq R$, hence R is an element of the defining set $\{\, C \subseteq R \mid A \subseteq C,\, C \text{ is a positive cone} \,\}$. In particular this set is non-empty and hence the intersection over all its elements exists.

(iii) Recall the definitions of the image $\varphi(C) = \{\, \varphi(a) \mid a \in C \,\}$ and the preimage $\varphi^{-1}(D) = \{\, a \in R \mid \varphi(a) \in D \,\}$. Now, as $0 = \varphi(0)$ and $1 = \varphi(1)$ we get both $0,\, 1 \in \varphi(C)$ and $0,\, 1 \in \varphi^{-1}(D)$.

So given any $u,\, v \in \varphi(C)$ there are some $a,\, b \in C$ such that $u = \varphi(a)$ and $v = \varphi(b)$. Thereby $u+v = \varphi(a)+\varphi(b) = \varphi(a+b) \in \varphi(C)$ and likewise $u \cdot v = \varphi(a) \cdot \varphi(b) = \varphi(a \cdot b) \in \varphi(C)$ again. Altogether this means that $\varphi(C)$ is a positive cone again.

Similarly, if $a,\, b \in \varphi^{-1}(D)$ we have $\varphi(a),\, \varphi(b) \in D$ and therefore $\varphi(a+b) = \varphi(a)+\varphi(b) \in D$ which implies $a+b \in \varphi^{-1}(D)$. In complete analogy we find $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) \in D$ and hence $a \cdot b \in \varphi^{-1}(D)$. □

Proof of (1.86):

In (i) to (iv) there is nothing to prove - everything is either trivial or well-known. But we wish to give a short prove for (v): First of all, we have $0 \leq 0$ due to the reflexivity (O1) of $\leq$. Furthermore $0 \leq 1$ is property (P1) of $\leq$. Thereby $0,\, 1 \in R^+$. If now $a,\, b \in R^+$, then $0 \leq a$ and $0 \leq b$ and hence $0 \leq a+b$ and $0 \leq a \cdot b$ due to properties (P3) and (P4). But this again means $a+b$ and $a \cdot b \in R^+$ such that R^+ is a positive cone. Suppose $a \in R^+ \cap (-R^+)$ that is $0 \leq a$ and $0 \leq -a$. The latter is $0 \leq 0-a$ and hence $a \leq 0$ due to (P2). But as also $0 \leq a$ the anti-symmetry (O2) implies $a = 0$.

Claim number (vi) is fairly easy to see: first of all $0 = 0^2$ and $1 = 1^2$ such that $0, 1 \in \Delta$ is satisfied. Property (C2) of cones is satisfied trivially and for property (C3) we have to regard $a = a_1^2 + \cdots + a_m^2$ and $b = b_1^2 + \cdots + b_n^2 \in \Delta$. Then it is clear that also $ab \in \Delta$, as

$$ab \;=\; \sum_{i=1}^{m}\sum_{j=1}^{n} a_i^2 b_j^2 \;=\; \sum_{(i,j)=(1,1)}^{(m,n)} (a_i b_j)^2$$

We will now prove (vii) that $R[x]^+$ is a proper cone: As $0 \in R^+$ and $\mathrm{lc}(0) = 0$ we get $0 \in R[x]^+$ as well. Likewise $1 \in R[x]^+$. If now f and g are two polynomials in $R[x]^+$ then we have to show that $f+g$ and $f \cdot g$ are in $R[x]^+$ again. If one of them - say $f = 0$ - then $f + g = g$ and $f \cdot g = 0$ and hence there is nothing to prove. Otherwise let

$$\begin{aligned} f(x) &= a_m x^m + \cdots + a_k x^k \\ g(x) &= b_n x^n + \cdots + b_l x^l \end{aligned}$$

By assumption $f, g \in R[x]^+$ we have a_m and $b_n \geq 0$. Therefore, if $m = n$ then $\mathrm{lc}(f+g) = a_n + b_n \geq 0$. And if $m \neq n$, say $m < n$ then $\mathrm{lc}(f+g) = b_n \geq 0$. In any case we get $\mathrm{lc}(f+g) \geq 0$ and hence $f + g \in R[x]^+$ again. Also by definition of the multiplication in $R[x]$ we have

$$(f \cdot g)(x) \;=\; \sum_{u=0}^{\infty} \left(\sum_{p+q=u} f[p] \cdot g[q] \right) x^u$$

Thus if $u > m + n$ then either $p > m$ or $q = u - p > n$, in any case we have $f[p] \cdot g[q] = 0$. And for the same reason all combinations (p, q) with $p + q = u$ for $u = m + n$ yield $f[p] \cdot g[q] = 0$ except $f[m] \cdot g[n] = a_m \cdot b_n \neq 0$, as R is an integral domain. Hence $\mathrm{lc}(f \cdot g) = a_m \cdot b_n$ and as both have been positive, so is $\mathrm{lc}(f \cdot g) \geq 0$. And this again means $f \cdot g \in R[x]^+$ such that $R[x]^+$ is a positive cone as well. To prove that $R[x]^+$ is proper consider some $f \in R[x]$ such that $f \in R[x]^+$ and $-f \in R[x]^+$. Let $a := \mathrm{lc}(f)$ then this means $a \geq 0$ and $-a \geq 0$. But due to (v) this implies $a = 0$ (see above). And the only polynomial with $\mathrm{lc}(f) = 0$ is $f = 0$.
In complete analogy to the arguments above one can show that $R[x]^-$ is a proper, positive cone of $R[x]$, as well. □

Proof of (1.89):

(i) If $a \geq 0$ then $|a| = a \geq 0$ is clear. Otherwise, if $a \leq 0$ then $|a| = -a$ but as $a \leq 0$ (P6) implies $-a \geq 0$ and hence $|a| \geq 0$.

(ii) If $a \geq 0$ then $|a| = a \geq a$ is clear. Otherwise, if $a \leq 0$ then $|a| = -a$ but as $a \leq 0$ (P6) implies $-a \geq 0 \geq a$ and hence $|a| \geq a$.

(iii) If $a \geq 0$ then $|a| = a$ and hence $|a|^2 = a^2$ is clear. Otherwise, if $a \leq 0$ then $|a| = -a$ such that $|a|^2 = (-a)^2 = a^2$ again.

(iv) We have to consider three cases: (1) if $a > 0$ then $|a| = a$ and $\mathrm{sgn}(a) = 1$ such that $|a| = a = 1 \cdot a = \mathrm{sgn}(a)a$. (2) if $a = 0$, then $|a| = 0$ and $\mathrm{sgn}(a) = 0$ such that $|a| = 0 = 0 \cdot 0 = \mathrm{sgn}(a)a$. (3) lastly, if $a < 0$ then $|a| = -a$ and $\mathrm{sgn}(a) = -1$ such that $|a| = -a = (-1) \cdot a = \mathrm{sgn}(a)a$. Thus the equality holds true in any of these three cases.

(ix) If $a \leq b$ then (as $0 \leq a$) we get $a^2 \leq ab$ due to (P8). Likewise (as $0 \leq b$ as well) we find $ab \leq b^2$. Thus $a^2 \leq ab \leq b^2$ which implies $a^2 \leq b^2$ due to the transitivity of $\leq$. Conversely we start with $a^2 \leq b^2$. Suppose we had $a > b$ then in particular $b \leq a$ such that $b^2 \leq a^2 \leq b^2$. This implies $a^2 = b^2$ and hence $0 = b^2 - a^2 = (a-b)(a+b)$. As R is an integral domain this would mean $a = b$ (in contradiction to $a > b$) or $a + b = 0$. But again $0 \leq a = -b \leq 0$ implies $a = b = 0$ in contradiction to $a > b$. Thus $a > b$ is false, which only leaves $a \leq b$.

(viii) If $a = 0$ or $b = 0$ then $ab = 0$ and hence $\operatorname{sgn}(ab) = 0 = \operatorname{sgn}(a)\operatorname{sgn}(b)$. Now suppose $a \neq 0$ and $b \neq 0$ and distinguish 4 cases: (1) if $a > 0$ and $b > 0$ then $ab > 0$ due to (P4) and hence $\operatorname{sgn}(ab) = 1 = 1 \cdot 1 = \operatorname{sgn}(a)\operatorname{sgn}(b)$. (2) if $0 < a$ and $b < 0$ then $0 > ab$ due to (P9) such that $\operatorname{sgn}(ab) = -1 = 1 \cdot (-1) = \operatorname{sgn}(a)\operatorname{sgn}(b)$. (3) the case $a < 0$ and $b > 0$ is completely analogous to case (2), by flipping a and b. (4) if $a < 0$ and $b < 0$ then $-a > 0$ and $-b > 0$. Now by (1) we get $\operatorname{sgn}(ab) = \operatorname{sgn}((-a)(-b)) = 1 = (-1)(-1) = \operatorname{sgn}(a)\operatorname{sgn}(b)$. Thus the equality holds true in any of these cases.

(v) Once (iv) and (viii) have been established this is straightforward: $|ab| = \operatorname{sgn}(ab)ab = \operatorname{sgn}(a)a \cdot \operatorname{sgn}(b)b = |a| \cdot |b|$.

(vi) Due to (iii) we know $|a+b|^2 = (a+b)^2 = a^2 + 2ab + b^2$. But according to (ii) $ab \leq |ab|$ such that $|a+b|^2 = a^2 + 2ab + b^2 \leq a^2 + 2|ab| + b^2$. We now invoke (v) and (iii) again to find $|a+b|^2 \leq a^2 + 2|ab| + b^2 = |a|^2 + 2|a||b| + |b|^2 = (|a| + |b|)^2$. As both $|a|$ and $|b| \geq 0$ we can finally use (ix) to deduce $|a+b| \leq |a| + |b|$ as claimed.

(vii) First of all $|a| = |b + (a-b)| \leq |b| + |a-b|$ according to (vi). And from this we get $|a| - |b| \leq |a-b|$. Now in complete analogy we have $|b| = |a + (b-a)| \leq |a| + |b-a|$ and hence $-(|a| - |b|) = |b| - |a| \leq |b-a| = |a-b|$. Combining these two cases we see $||a| - |b|| \leq |a-b|$.

□

Proof of (1.91):
First of all for any $a \in R$ we have $a - a = 0 \in C$ and hence (O1). Also if $a \leq b$ and $b \leq c$ this means $b - a$ and $c - b \in C$ and hence $c - a = (c-b) + (b-a) \in C$ such that (O2). In particular, if $a \leq b$ and $b \leq a$ that $b - a$ and $-(b-a) = a - b \in C$, but as C is proper this means $b - a = 0$ and hence (O3). As $1 \in C$ we have $0 \leq 1$ which is (P1), (P2) is satisfied trivially: $a \leq b \iff b - a \in C \iff (b-a) - 0 \in C \iff 0 \leq b - a$. And at last, for any a and $b \in R$ with $0 \leq a$ and $0 \leq b$ we have a, $b \in C$ such that $a + b$ and $ab \in C$ which again means $a + b$ resp. $ab \geq 0$. □

Proof of (1.92):
We have already proved that: given a proper positive cone C we can define a positive order $a \leq b$ by letting $b - a \in C$. And conversely, if $\leq$ is a positive order on R, then $R^+ = \{\, a \in R \mid a \geq 0 \,\}$ is a proper positive cone in R. Hence both of these maps are well-defined. It remains to show that they also are mutually inverse.
Let us first start with a proper positive cone C, then we have to show that $R^+ = C$. By definition $a \geq 0$ means $a - 0 = a \in C$, so this is true already. Conversely, given a positive order $\leq$ we have to show that $a \leq b$ is equivalent to $b - a \in R^+$. But by definition this is $b - a \geq 0$ such that this is guaranteed by property (P2) of positive orders. □

Proof of (1.93):
A word in advance: we have $N = R^+ \cap \mathrm{NZD}(R)$. It is well known (and easy to see) that the set $\mathrm{NZD}(R)$ of non-zero divisors of R is multiplicatively closed. And R^+ is multiplicatively closed due to (1) and (4). Hence N is multiplicatively closed, as an intersection of such sets.
To begin with we have to prove the well-definedness of the relation. Thus we consider $a/m = a'/m'$ and $b/n = b'/n'$. That is $u(am' - a'm) = 0$ for some $u \in N$. In particular u is a non-zero divisor and hence $am' = a'm$. Likewise $bn' = b'n$. We now have to show that $a'/m' \leq b'/n'$ implies (and by universality hence already is equivalent to) $a/m \leq b/n$. By definition

$$\frac{a'}{m'} \leq \frac{b'}{n'} \iff a'n' \leq b'm' \iff 0 \leq b'm' - a'n'$$

Multiplying the latter inequality with $mn \geq 0$ we get $0 \leq mn(b'm' - a'n') = b'nmm' - a'mnn' = bn'mm' - am'nn'$. This again yields $am'nn' \leq bn'mm'$, which once again iturns into

$$a(nm'n') \leq (bm'n')m \iff \frac{a}{m} \leq \frac{bm'n'}{nm'n'} = \frac{b}{n}$$

Thus we truly got $a/m \leq b/n$ and hence the well-definedness of $\leq$. In a next step we have to prove that this relation also is a partial order. The *reflexivity* $a/m \leq a/m$ is clear, as $am \leq am$. The *anti-symmetry* is easy as well: consider $a/m \leq b/n$ such that $a/m \leq b/n$ as well. This means $an \leq bm$ and $bm \leq an$ such that $an = bm$. This again is $a/m = b/n$. It remains to verify the *transitivity*: consider $a/m \leq b/n$ and $b/n \leq c/u$. That is $an \leq bm$ and $bu \leq cn$. As u and $m \geq 0$ we find $aun \leq bum$ and $bum \leq cnm$ such that $aun \leq cnm$. This again yields $a/m \leq (cn)/(un) = c/u$.
Now we're ready for the actual topic of the claim: the *positivity* of the partial order $\leq$. First note that by definition we have

$$0 \leq \frac{b}{n} \iff 0 \leq b$$

Thereby property (1) is obvious, as $0/1 \leq 1/1 \iff 0 \leq 1$. And for (2) we consider $a/m \leq b/n$, which is $an \leq bm$ and hence $0 \leq bm - an$. As we have just seen this is $0 \leq (bm - an)/(mn) = b/n - a/m$, such that the equivalence is established. For properties (3) and (4) we are given a/m and $b/n \geq 0$. That is a, $b \geq 0$, hence $ab \geq 0$ and thus $(a/m)(b/n) = (ab)/(mn) \geq 0$. Likewise (as m, $n \geq 0$ as well) we have $an + bm \geq 0$ such that $a/m + b/n = (an + bm)/(mn) \geq 0$. □

Proof of (1.97):

(1) We will first prove that $\mathfrak{a} \oplus \mathfrak{b} \trianglelefteq_{\mathrm{i}} R \oplus S$ is an ideal. As $\mathfrak{a}$ and $\mathfrak{b}$ are ideals we have $0 \in \mathfrak{a}$ and $0 \in \mathfrak{b}$ and hence $0 = (0,0) \in \mathfrak{a} \oplus \mathfrak{b}$. Now consider (a,b) and $(p,q) \in \mathfrak{a} \oplus \mathfrak{b}$. Then we have $a + p \in \mathfrak{a}$, $b + q \in \mathfrak{b}$ and hence $(a,b) + (p,q) = (a + p, b + q) \in \mathfrak{a} \oplus \mathfrak{b}$. Finally consider any $(r,s) \in R \oplus S$ then $ra \in \mathfrak{a}$ and $sb \in \mathfrak{b}$ such that $(r,s)(a,b) = (ra,sb) \in \mathfrak{a} \oplus \mathfrak{b}$ again. And as R and S are commutative rings, so is $R \oplus S$ such that this has been enough to guarantee that $\mathfrak{a} \oplus \mathfrak{b}$ is an ideal of $R \oplus S$.

(2) Next we will prove $\mathfrak{u} = \varrho(\mathfrak{u}) \oplus \sigma(\mathfrak{u})$. If $(a,b) \in \mathfrak{u}$ then it is clear that $a = \varrho(a,b) \in \varrho(\mathfrak{u})$ and $b = \sigma(a,b) \in \sigma(\mathfrak{u})$ such that $(a,b) \in \varrho(\mathfrak{u}) \oplus \sigma(\mathfrak{u})$. Conversely if $(a,b) \in \varrho(\mathfrak{u}) \oplus \sigma(\mathfrak{u})$ then there are some $r \in R$ and $s \in S$ such that $(a,s) \in \mathfrak{u}$ and $(r,b) \in \mathfrak{u}$. But as $\mathfrak{u}$ is an ideal we also have $(a,0) = (1,0)(a,s) \in \mathfrak{u}$ again and analogously $(0,b) \in \mathfrak{u}$. Thererby $(a,b) = (a,0) + (0,b) \in \mathfrak{u}$ proving the equality.

(3) Now we are ready to prove $\mathrm{Ideal}(R) \oplus S = \{\mathfrak{a} \oplus \mathfrak{b} \mid \mathfrak{a} \trianglelefteq_{\mathrm{i}} R,\ \mathfrak{b} \trianglelefteq_{\mathrm{i}} S\}$. We have already seen in (1) that $\mathfrak{a} \oplus \mathfrak{b}$ is an ideal of $R \oplus S$ (supposed $\mathfrak{a}$ and $\mathfrak{b}$ are ideals). Conversely if $\mathfrak{u} \trianglelefteq_{\mathrm{i}} R \oplus S$ is an ideal, then we let $\mathfrak{a} := \varrho(\mathfrak{u})$ and $\mathfrak{b} := \sigma(\mathfrak{u})$. Then $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ and $\mathfrak{b} \trianglelefteq_{\mathrm{i}} S$ are ideals, since ϱ and σ are surjective homomorphisms. And $\mathfrak{u} = \mathfrak{a} \oplus \mathfrak{b}$ by (2).

(4) Now let $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ and $\mathfrak{b} \trianglelefteq_{\mathrm{i}} S$. Then we will prove $\sqrt{\mathfrak{a} \oplus \mathfrak{b}} = \sqrt{\mathfrak{a}} \oplus \sqrt{\mathfrak{b}}$. First suppose that $(a,b)^k = (a^k, b^k) \in \mathfrak{a} \oplus \mathfrak{b}$ for some $k \in \mathbb{N}$. Then $a^k \in \mathfrak{a}$ and $b^k \in \mathfrak{b}$ such that $a \in \sqrt{\mathfrak{a}}$ and $b \in \sqrt{\mathfrak{b}}$ and thereby $(a,b) \in \sqrt{\mathfrak{a}} \oplus \sqrt{\mathfrak{b}}$. Conversely suppose $a^k \in \mathfrak{a}$ and $b^l \in \mathfrak{b}$ for some $k, l \in \mathbb{N}$. Then we define $n := \max\{k,l\}$ and thereby get $(a,b)^n = (a^n, b^n) \in \mathfrak{a} \oplus \mathfrak{b}$. And this means that (a,b) is contained in the radical of $\mathfrak{a} \oplus \mathfrak{b}$ again.

(5) This enables us to prove $\mathrm{Srad}(R) \oplus S = \{\mathfrak{a} \oplus \mathfrak{b} \mid \mathfrak{a} = \sqrt{\mathfrak{a}},\ \mathfrak{b} = \sqrt{\mathfrak{b}}\}$. First suppose that $\mathfrak{u} \trianglelefteq_{\mathrm{i}} R \oplus S$ is a radical ideal and let $\mathfrak{a} := \varrho(\mathfrak{u})$ and $\mathfrak{b} := \sigma(\mathfrak{u})$ again. Then by (4) we may compute

$$\mathfrak{a} \oplus \mathfrak{b} \;=\; \mathfrak{u} \;=\; \sqrt{\mathfrak{u}} \;=\; \sqrt{\mathfrak{a} \oplus \mathfrak{b}} \;=\; \sqrt{\mathfrak{a}} \oplus \sqrt{\mathfrak{b}}$$

This proves that $\mathfrak{a} = \sqrt{\mathfrak{a}}$ and $\mathfrak{b} = \sqrt{\mathfrak{b}}$ are radical ideals of R and S respectively. And if conversely $\mathfrak{a}$ and $\mathfrak{b}$ are radical ideals then $\mathfrak{a} \oplus \mathfrak{b}$ is a radical ideal of $R \oplus S$ by virtue of

$$\mathfrak{a} \oplus \mathfrak{b} \;=\; \sqrt{\mathfrak{a}} \oplus \sqrt{\mathfrak{b}} \;=\; \sqrt{\mathfrak{a} \oplus \mathfrak{b}}$$

(6) Next we will prove $\mathrm{Spec}(R) \oplus S = \{\mathfrak{p} \oplus S\} \cup \{R \oplus \mathfrak{q}\}$. If $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ is a prime ideal then we have already proved $\mathfrak{p} \oplus S \trianglelefteq_{\mathrm{i}} R \oplus S$ in (1). And it is clear that $\mathfrak{p} \oplus S \neq R \oplus S$ as $(1,0) \notin \mathfrak{p} \oplus S$. Thus suppose $(a,b)(p,q) = (ap, bq) \in \mathfrak{p} \oplus S$. Then $ap \in \mathfrak{p}$ and as $\mathfrak{p}$ is prime this means $a \in \mathfrak{p}$ or $p \in \mathfrak{p}$. Without loss of generality we may take $p \in \mathfrak{p}$ and thereby $(p,q) \in \mathfrak{p} \oplus S$. Altogether we have seen that $\mathfrak{p} \oplus S$ is a prime ideal of $R \oplus S$. And analogously one may prove that $R \oplus \mathfrak{q}$ is prime, supposed $\mathfrak{q} \trianglelefteq_{\mathrm{i}} S$ is prime. Thus conversely consider a prime ideal $\mathfrak{u} \trianglelefteq_{\mathrm{i}} R \oplus S$ let $\mathfrak{p} := \varrho(\mathfrak{u})$ and $\mathfrak{q} := \sigma(\mathfrak{u})$. Clearly $(1,0)(0,1) = (0,0) \in \mathfrak{u}$. And as $\mathfrak{u}$ is prime this means $(1,0) \in \mathfrak{u}$ or $(0,1) \in \mathfrak{u}$. We will assume $(0,1) \in \mathfrak{u}$, as the other case can be dealt with in complete analogy. Then $1 \in \mathfrak{q}$ and hence $\mathfrak{q} = S$. That is $\mathfrak{u} = \mathfrak{p} \oplus S$ and as $\mathfrak{u} \neq R \oplus S$ this means $\mathfrak{p} \neq R$. Thus consider a and $p \in R$ such that $ap \in \mathfrak{p}$. Then $(a,0)(p,0) = (ap,0) \in \mathfrak{p} \oplus S = \mathfrak{u}$. And as $\mathfrak{u}$ is prime this means $(a,0) \in \mathfrak{u}$ or $(p,0) \in \mathfrak{u}$ (which we assume w.l.o.g.). Thereby $p \in \mathfrak{p}$, altogether we have found that $\mathfrak{u} = \mathfrak{p} \oplus S$ for some prime ideal $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$.

(7) It remains to prove $\mathrm{Smax}(R) \oplus S = \{\mathfrak{m} \oplus S\} \cup \{R \oplus \mathfrak{n}\}$. Thus consider a maximal ideal $\mathfrak{m} \trianglelefteq_{\mathrm{i}} R$ and suppose $\mathfrak{m} \oplus S \subseteq \mathfrak{u} \trianglelefteq_{\mathrm{i}} R \oplus S$. Then $S = \sigma(\mathfrak{m} \oplus S) \subseteq \mathfrak{b} := \sigma(\mathfrak{u}) \trianglelefteq_{\mathrm{i}} S$ and hence $\mathfrak{b} = S$. Likewise we find $\mathfrak{m} = \varrho(\mathfrak{m} \oplus S) \subseteq \mathfrak{a} := \varrho(\mathfrak{u}) \trianglelefteq_{\mathrm{i}} R$ and as $\mathfrak{m}$ is maximal this implies $\mathfrak{a} = \mathfrak{m}$ or $\mathfrak{a} = R$. Thus we get $\mathfrak{u} = \mathfrak{a} \oplus \mathfrak{b} = \mathfrak{m} \oplus S$ or $\mathfrak{u} = \mathfrak{a} \oplus \mathfrak{b} = R \oplus S$. And this means that $\mathfrak{m} \oplus S$ is a maximal ideal of $R \oplus S$. Likewise one can see that $R \oplus \mathfrak{n}$ is a maximal ideal for any $\mathfrak{n} \trianglelefteq_{\mathrm{i}} S$ maximal. Conversely consider a maximal ideal $\mathfrak{u} \trianglelefteq_{\mathrm{i}} R \oplus S$. In particular $\mathfrak{u}$ is prime and hence - by (6) - $\mathfrak{u} = \mathfrak{m} \oplus S$ or $\mathfrak{u} = R \oplus \mathfrak{n}$ for some prime ideal $\mathfrak{m} \trianglelefteq_{\mathrm{i}} R$ or $\mathfrak{n} \trianglelefteq_{\mathrm{i}} S$ respectively. We only regard the case $\mathfrak{u} = \mathfrak{m} \oplus S$ again, as the other is completely analogous. Thus consider some ideal $\mathfrak{m} \subseteq \mathfrak{a} \trianglelefteq_{\mathrm{i}} R$, then $\mathfrak{u} = \mathfrak{m} \oplus S \subseteq \mathfrak{a} \oplus S \trianglelefteq_{\mathrm{i}} R \oplus S$. By maximality of $\mathfrak{u}$ that is $\mathfrak{u} = \mathfrak{m} \oplus S = \mathfrak{a} \oplus S$ or $\mathfrak{a} \oplus S = R \oplus S$. Again this yields $\mathfrak{m} = \mathfrak{a}$ or $\mathfrak{a} = R$ and this means that $\mathfrak{m}$ is maximal.

□

Proof of (1.99):

(i) From $1 = e + f \in \mathfrak{a} + \mathfrak{b} \trianglelefteq_{\mathfrak{i}} R$ it is clear that $\mathfrak{a} + \mathfrak{b} = R$. Now consider any $x \in \mathfrak{a} \cap \mathfrak{b}$. That is there are a and $b \in R$ such that $x = ae = bf$. Then we get $xe = (bf)e = b(fe) = 0$ and $xf = (ae)f = a(ef) = 0$. And thereby $x = x1 = x(e + f) = xe + xf = 0$ such that $\mathfrak{a} \cap \mathfrak{b} = \{0\}$.

(ii) For any $a \in R$ we have $a = a1 = a(e_1 + \cdots + e_n) = ae_1 + \cdots + ae_n \in \mathfrak{a}_1 + \cdots + \mathfrak{a}_n$. Thus we have $R \subseteq \mathfrak{a}_1 + \cdots + \mathfrak{a}_n$ and the converse inclusion is clear, as all the $\mathfrak{a}_k$ are ideals of R. That is property (1). For (2) we consider any $x \in \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n$. That is for any $i \in 1 \ldots n$ there is some $a_i \in R$, such that $x = a_i e_i$. Thus for any $j \neq i$ we get $xe_j = (ae_i)e_j = a(e_i e_j) = 0$. As $n \geq 2$ we may choose $xe_1 = (a_2 e_2)e_1 = 0$ and for any $j \geq 2$ likewise $xe_j = (a_1 e_1)e_j = 0$. Thereby we find $x = x1 = x(e_1 + \cdots + e_n) = xe_1 + \cdots + xe_n = 0$. That is property (2).

(iii) It is clear that $\Phi : x \mapsto (x + \mathfrak{a}, x + \mathfrak{b})$ is a well-defined homomorphism of rings (as it fibers into the canonical epimorphisms $x \mapsto x + \mathfrak{a}$ and $x \mapsto x + \mathfrak{b}$). Now suppose $(x + \mathfrak{a}, x + \mathfrak{b}) = \Phi(x) = 0 = (0 + \mathfrak{a}, 0 + \mathfrak{b})$. This means $x \in \mathfrak{a}$ and $x \in \mathfrak{b}$ and hence $x \in \mathfrak{a} \cap \mathfrak{b} = \{0\}$. Thus we have $x = 0$ which implies $\mathrm{kn}(\Phi) = \{0\}$, which means that Φ is injective. It remains to prove, that Φ also is surjective: Since $\mathfrak{a} + \mathfrak{b} = R$ there are some $e \in \mathfrak{a}$ and $f \in \mathfrak{b}$ such that $e + f = 1$. Now suppose we are given any $(y + \mathfrak{a}, z + \mathfrak{b})$. Then let $x := yf + ze$ and compute

$$\begin{aligned}
\Phi(x) &= (yf + ze + \mathfrak{a}, yf + ze + \mathfrak{b}) \\
&= (yf + \mathfrak{a}, ze + \mathfrak{b}) \\
&= (yf + ye + \mathfrak{a}, ze + zf + \mathfrak{b}) \\
&= (y(f + e) + \mathfrak{a}, z(e + f) + \mathfrak{b}) \\
&= (y + \mathfrak{a}, z + \mathfrak{b})
\end{aligned}$$

(iv) We will now prove the Chinese remainder theorem in several steps. (1) Let us first consider the following homomorphism of rings

$$\varphi \ : \ R \to \bigoplus_{i=1}^{n} R \Big/ \mathfrak{a}_i \ : \ x \mapsto (x + \mathfrak{a}_i)$$

We now compute the kernel of φ: $\varphi(x) = 0 = (0 + \mathfrak{a}_i)$ holds true if and only if for any $i \in 1 \ldots n$ we have $x + \mathfrak{a}_i = 0 + \mathfrak{a}_i$. And of course this is equivalent, to $x \in \mathfrak{a}_i$ for any $i \in 1 \ldots n$. And again this can be put as $x \in \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n$. Hence we found $\mathrm{kn}(\varphi) = \mathfrak{a}$. Now we aim for the surjectivity of φ: (2) As a first approach we prove the existence of a solution $x \in R$ of the system $\varphi(x) = (1 + \mathfrak{a}_1, 0 + \mathfrak{a}_2, \ldots, 0 + \mathfrak{a}_n)$. Since $\mathfrak{a}_1 + \mathfrak{a}_j = R$ for any $j \in 2 \ldots n$ we also find $\mathfrak{a}_1 + \mathfrak{a}_2 \ldots \mathfrak{a}_n = R$ due to (1.61.(iii)). That is there are elements $e_1 \in \mathfrak{a}_1$ and $f_1 \in \mathfrak{a}_2 \ldots \mathfrak{a}_n$ such that $e_1 + f_1 = 1$. Hence we find $f_1 + \mathfrak{a}_j = 0 + \mathfrak{a}_j$ for any $j \in 2 \ldots n$. And also $f_1 + \mathfrak{a}_1 = (1 - e_1) + \mathfrak{a}_1 = 1 + \mathfrak{a}_1$. That is $x := f_1$ does the trick. (3) Analogous to (2) we find $f_2, \ldots, f_n \in R$ such that for any $j \in 1 \ldots n$ we obtain the system

$$\varphi(f_j) \ = \ (\delta_{i,j} + \mathfrak{a}_i)$$

(4) Thus if we are now given any $a_1, \ldots, a_n \in R$ then we let us define $x := a_1 f_1 + \cdots + a_n f_n$ and

we thereby obtain

$$x + \mathfrak{a}_i \;=\; \sum_{j=1}^{n} a_j f_j + \mathfrak{a}_i \;=\; \sum_{j=1}^{n} a_j \delta_{i,j} + \mathfrak{a}_i \;=\; a_j + \mathfrak{a}_i$$

Hence $\varphi(x) = (a_i + \mathfrak{a}_i)$ and as the a_i have been arbitrary this means that φ is surjective. (5) Thus (1.83.(ii)) yields the desired isomorphy.

□

15.3 Proofs of Chapter 2

Proof of (2.1):

(v) As $\leq$ is a total order, we may assume $a \leq b$ without loss of generality. If $a, b \in A^*$, then $b \in A$, $a \leq b$ and $a \in A^*$ implies $a = b$. Likewise if $a, b \in A_*$ then $a \in A$, $a \leq b$ and $a \in A_*$ implies $a = b$.

(vi) By induction on n: if $n = 1$ then $a_* = a_1$ is trivial and if $n = 2$ then a_* is minimal by construction. Thus for $n \geq 3$ we let $H := \{ a_1, \ldots, a_{n-1} \} \subseteq A$. By induction hypothesis we have $H_* = \{ h_* \}$ for $h^* = ((a_1 \wedge a_2) \ldots) \wedge a_{n-1}$. Now let $a_* := h_* \wedge a_n$ then $a_* \leq h_* \leq a_i$ for $i < n$ and $a_* \leq a_n$ by construction. Hence we have $a_* \leq a_i$ for any $i \in 1 \ldots n$, which means $a_* \in A_*$. And the uniqueness has already been shown above. This also proves the like statement for A^* by taking to the inverse ordering $b \geq a \ :\Longleftrightarrow \ a \leq b$.

(ix) Regard $\mathcal{Z}$ as a partially ordered set $(\mathcal{Z}, \subseteq)$ under the inclusion relation (this is allowed, due to (1)). If now $\mathcal{C} \subseteq \mathcal{Z}$ is a chain, then by (2) we get $U := \bigcup \mathcal{C} \in \mathcal{Z}$. And clearly we have $C \subseteq U$ for any $C \in \mathcal{C}$. Thus U is an upper bound of $\mathcal{C}$ and hence we may apply the lemma of Zorn to $(\mathcal{Z}, \subseteq)$, to find a maximal element $Z \in \mathcal{Z}^*$.

(x) Let us define the partial order $B \leq A \ :\Longleftrightarrow \ A \subseteq B$ on $\mathcal{Z}$. If now $\mathcal{C} \subseteq \mathcal{Z}$ is a chain, then by (2) we get $U := \bigcap \mathcal{C} \in \mathcal{Z}$. And clearly $U \subseteq C$ (which translates into $C \leq U$) for any $C \in \mathcal{C}$. Thus U is an upper bound of $\mathcal{C}$ and hence we may apply the lemma of Zorn to find a $\leq$-maximal element Z. But being $\leq$-maximal trivially translates into being $\subseteq$-minimal again.

□

Proof of (2.67):
Existence: Let us abbreviate $m := \deg(f)$ and $n := \deg(g)$. If $n < m$ then we may take $q = 0$ and $r = g$ and are done already. Thus throughout this proof we may assume $m \leq n$. We will now use induction on n: In case $n = 0$ we have $g = g[0] \in R$ and since $m \leq n = 0$ also $f = f[0] = 1$. Thus the claim is trivially satisfied, with $r = 0$ and $q = g[0]$, since

$$g \ = \ g[0] \ = \ g[0] \cdot 1 + 0 \ = \ qf + r$$

So let us now assume, we had some q and r as required for any polynomial of degree up to $n-1$. Then we need to find sufficient polynomials for g of degree n. To find these let

$$p \ := \ g[n] t^{n-m} \ \in \ R[t]$$

Then it is clear that $\deg(g - pf) < n$ since

$$\begin{aligned} g - pf &= \sum_{k=0}^{n} g[k] t^k - g[n] t^{n-m} \left(t^m + \sum_{k=0}^{m-1} f[k] t^k \right) \\ &= \sum_{k=0}^{n} g[k] t^k - g[n] t^n - \sum_{k=0}^{m-1} g[n] f[k] t^{n-m+k} \end{aligned}$$

$$= \sum_{k=0}^{n-1} g[k]t^k - \sum_{k=n-m}^{n-1} g[n]f[k-n+m]t^k$$

Thus by induction hypothesis there are some q_0, $r \in R$ with $g - pf = q_0 f + r$ and $\deg(g) < \deg(f)$. But from this equation we find $g = (p + q_0)f + r$ such that we may take $q = q_0 + p$ and r as the required polynomials in the induction step.

Uniqueness: Hereby R is an integral domain. Suppose we had two decompositions $g = pf + r$ and $g = qf + s$, where $r = 0$ or $\deg(r) < \deg(f)$ and $s = 0$ or $\deg(s) < \deg(f)$. Note that these equations can be rewritten, as

$$(q-p)f - (r-s) \; = (qf+s) - (pf+r) \; = \; g - g \; = \; 0$$

This means $(q-p)f = r - s$ But $\deg(r-s) < \deg(f)$ as both r and s are of lower degree. Suppose $q - p \neq 0$ then $\deg((q-p)f) \geq \deg(f)$, since R is an integral domain. But as $\deg((q-p)f) = \deg(r-s) < \deg(f)$ this cannot be. This only leaves the possibility $q - p = 0$ (that is $p = q$) and thereby also $r - s = (q-p)f = 0$ (that is $r = s$). □

15.4 Proofs of Chapter 3

Proof of (3.10):

- First suppose M is an R-module and $P_i \leq_{\mathsf{m}} M$ are R-sub-modules and let $P := \bigcap_i P_i \subseteq M$. In particular we get $0 \in P_i$ for any $i \in I$ and hence $0 \in P$. And if we are given any $x, y \in P$ this means $x, y \in P_i$ for any $i \in I$. And as any $P_i \leq_{\mathsf{m}} M$ is an R-sub-module this implies $x + y \in P_i$ which is $x + y \in P$ again, as i has been arbitrary. Likewise consider any $a \in R$, then $ax_i \in P_i$ again and hence $ax \in P$. Altogether $P \leq_{\mathsf{m}} M$ is an R-sub-module of M.

- Now suppose M is an R-semi-algebra and $P_i \leq_{\mathsf{b}} A$ are R-sub-semi-algebras and let $P := \bigcap_i P_i \subseteq M$ again. In particular $P_i \leq_{\mathsf{m}} M$ and, as we have already seen, this implies $P \leq_{\mathsf{m}} M$. Thus consider any $f, g \in P$ that is $f, g \in P_i$ for any $i \in I$. As any P_i is an R-sub-semi-algebra we get $fg \in P_i$ again and hence $fg \in P$, as i has been arbitrary. Thus P is an R-sub-semi-algebra again.

- Next suppose M is an R-algebra with unit element 1, $P_i \leq_{\mathsf{a}} M$ are R-subalgebras and let $P := \bigcap P_i$ once more. Then we have just seen that $P \leq_{\mathsf{b}} M$ again. But as $P_i \leq_{\mathsf{a}} M$ we have $1 \in P_i$ again. And as this is true for any $i \in I$ this implies $1 \in P$, such that $P \leq_{\mathsf{a}} M$.

- Finally consider the R-semi-algebra A and the R-algebra-ideals $\mathfrak{a}_i \trianglelefteq_{\mathsf{a}} A$ and let $\mathfrak{a} := \bigcap_i \mathfrak{a}_i \subseteq A$. As our first claim we have already shown $\mathfrak{a} \leq_{\mathsf{m}} A$, thus consider any $f \in \mathfrak{a}$ and any $g \in M$. Then we have $f \in \mathfrak{a}_i$ for any $i \in I$ and as this is an R-sub-semi-algebra this implies fg and $gf \in \mathfrak{a}_i$ again. And as i is arbitrary this finally is fg and $gf \in \mathfrak{a}$ such that $\mathfrak{a} \trianglelefteq_{\mathsf{a}} A$, again.

□

Proof of (3.12):

- Let us denote the set $P := \{\sum_i a_i x_i\}$ of which we claim $P = \langle X \rangle_{\mathsf{m}}$. First of all it is clear that $X \subseteq P$, as $x = 1x \in P$ for any $x \in X$. Further it is clear that $P \leq_{\mathsf{m}} M$ is a sub-module of M: choose any $x \in X$, then $0 = 0 \diamond x \in P$, and if $a \in R$, $x = a_1 x_1 + \cdots + a_m x_m$ and $y = b_1 y_1 + \cdots + b_n y_n \in P$ then $ax = (aa_1)x_1 + \cdots + (aa_m)x_m \in P$ and $x + y = a_1 x_1 + \cdots + a_m x_m + b_1 y_1 + \cdots + b_n y_n \in P$. Thus by definition of $\langle X \rangle_{\mathsf{m}}$ we get $\langle X \rangle_{\mathsf{m}} \subseteq P$. Now suppose $Q \leq_{\mathsf{m}} M$ is any sub-module of M containing $X \subseteq Q$. Then for any $a_i \in R$ and any $x_i \in X \subseteq Q$ we get $a_i x_i \in Q$ and hence $\sum_i a_i x_i \in Q$, too. That is $P \subseteq Q$, and as Q has been arbitrary this means $P \subseteq \langle X \rangle_{\mathsf{m}}$, by the definition of $\langle X \rangle_{\mathsf{m}}$.

- Denote the set $P := \{\sum_i a_i \prod_j x_{i,j}\}$ of which we claim $P = \langle X \rangle_{\mathsf{b}}$. Again it is clear, that $X \subseteq P$, as $x = 1x \in P$ for any $x \in X$. Further it is clear that $P \leq_{\mathsf{b}} A$ is a sub-semi-algebra of A: choose any $x \in X$, then $0 = 0 \diamond x \in P$, and if $a \in R$, $f = \sum_i a_i \prod_j x_{i,j}$ and $g = \sum_k b_k \prod_l y_{k,l}$, then $af = \sum_i (aa_i) \prod_j x_{i,j} \in P$, $f + g = \sum_i a_i \prod_j x_{i,j} + \sum_k b_k \prod_l y_{k,l} \in P$ and by general distributivity $fg = \sum_i \sum_j (a_i b_j)(\prod_j x_{i,j} \prod_l y_{k,l}) \in P$. Thus by definition of $\langle X \rangle_{\mathsf{b}}$ we get $\langle X \rangle_{\mathsf{b}} \subseteq P$. Now suppose $Q \leq_{\mathsf{b}} A$ is any sub-semi-algebra of A. Then for any $a_i \in R$ and any $x_{i,j} \in X \subseteq Q$ we get $\prod_j x_{i,j} \in Q$, hence $a_i \prod_j x_{i,j} \in Q$ and finally $\sum_i a_i \prod_j x_{i,j} \in Q$. That is $P \subseteq Q$, and as Q has been arbitrary, this means $P \subseteq \langle X \rangle_{\mathsf{b}}$, by definition of $\langle X \rangle_{\mathsf{b}}$.

- By construction $P := \langle X \cup \{1\} \rangle_{\mathsf{b}}$ is a sub-semi-algeba containing 1, in other words a subalgebra. And as $X \subseteq P$ this implies $\langle X \rangle_{\mathsf{a}} \subseteq P$. And as any subalgebra $Q \leq_{\mathsf{a}} A$ contains 1 we get the

implications $X \subseteq Q \implies X \cup \{1\} \subseteq Q \implies P \subseteq Q$. This also proves $\langle X \rangle_{\mathfrak{a}} \subseteq P$, as Q has been arbitrary.

□

Proof of (3.14):

- We first prove that $\sim$ truly is an equivalence relation, the *reflexivity* $x \sim x$ is clear, as $x - x = 0 \in P$. For the *symmetry* suppose $x \sim y$, that is $y - x \in P$ and hence $x - y = -(y - x) = (-1)(y - x) \in P$. For the *transitivity* we finally consider $x \sim y$ and $y \sim z$. That is $y - x \in P$ and $z - y \in P$ and this yields $z - x = (z - y) + (y - x) \in P$. As in the proof of (1.62) it is clear that $[x] = x + P$, as

$$[x] \;=\; \{\, y \in M \mid y - x \in P \,\} \;=\; x + P$$

- Next we will prove the well-definedness of the addition and scalar-multiplication. Thus consider $x + P = x' + P$ and $y + P = y' + P$, that is $x' - x \in P$ and $y' - y \in P$. As P is an R-sub-module we get $(x' + y') - (x + y) = (x' - x) + (y' - y) \in P$ and this again is $(x + y) + P = (x' + y') + P$. Likewise for any $a \in R$ we get $(ax') - (ax) = a(x' - x) \in P$, which is $ax + P = ax' + P$.

- Now we immediately see, that M/P is an R-module again. The associativity and commutativity of $+$ are inherited trivially from M. And the same is true for the compatibility properties of $\diamond$. The neutral element of M/P is given to be $0 + P$, as for any $x + P \in M/P$ we get $(x + P) + (0 + P) = (x + 0) + P = x + P$. And the inverse of $x + P \in M/P$ is just $(-x) + P$, as $(x + P) + ((-x) + P) = (x + (-x)) + P = 0 + P$.

- Finally suppose A is an R-(semi)algebra, then we want to show that $A/\mathfrak{a}$ is an R-(semi)algebra again. As the R-algebraideal $\mathfrak{a}$ is an R-sub-module $A/\mathfrak{a}$ already is an R-module, by what we have already shown. Next we have to verify the well-definedness of the multiplication. Thus consider $f + \mathfrak{a} = f' + \mathfrak{a}$ and $g + \mathfrak{a} = g' + \mathfrak{a}$, then $(f'g') - (fg) = f'(g' - g) + (f' - f)g \in \mathfrak{a}$, by assumption on $\mathfrak{a}$. Now it is clear that $A/\mathfrak{a}$ inherits the associativity of the multiplication from A. Likewise the compatibility properties of $\cdot$, $+$ and $\diamond$ are inherited trivially. As an example let us regard the identity of

$$\begin{aligned}
\Big(a(f + \mathfrak{a})\Big)(g + \mathfrak{a}) &= (af + \mathfrak{a})(g + \mathfrak{a}) = (af)g + \mathfrak{a} = a(fg) + \mathfrak{a} \\
(f + \mathfrak{a})\Big(a(g + \mathfrak{a})\Big) &= (f + \mathfrak{a})(ag + \mathfrak{a}) = f(ag) + \mathfrak{a} = a(fg) + \mathfrak{a} \\
a\Big((f + \mathfrak{a})(g + \mathfrak{a})\Big) &= a(fg + \mathfrak{a}) = a(fg) + \mathfrak{a}
\end{aligned}$$

□

Proof of (3.16):

(i) We will first prove the equivalence $x + L \in P/L \iff x \in P$. The one implication is trivial: if $x \in P$, then $x + L \in P/L$ by definition. Conversely suppose there is some $p \in P$ such that $x + L = p + L \in P/L$. By definition of M/L this means $x - p \in L$, that is $x - p = \ell$ for some $\ell \in L \subseteq P$. And therefore $x = p + \ell \in P$, as $p, \ell \in P$ and $P \leq_{\mathfrak{m}} M$.

Now we are ready to prove $P/L \leq_{\mathsf{m}} M/L$, clearly $0 = 0 + L \in P/L$, as we have $0 \in P$. Now consider $x + L$ and $y + L \in P/L$, by what we have just seen this means x and $y \in P$. As $P \leq_{\mathsf{m}} M$ this implies $x + y \in P$ and hence $(x + L) + (y + L) = (x + y) + L \in P/L$ again. Finally consider any $a \in R$, as $x \in P$ and $P \leq_{\mathsf{m}} M$ this implies $ax \in P$ and hence also $a(x + L) = (ax) + L \in P/L$. Altogether P/L is a sub-module of M/L.

(ii) In (i) we have seen that $P \mapsto P/L$ is a well-defined map, so next we will point out that $U \mapsto (U) := \{ x \in M \mid x + L \in U \}$ is well-defined, too. That is we have to verify $(U) \leq_{\mathsf{m}} M$ and $L \subseteq (U)$. The containment $L \subseteq (U)$ is clear, if $\ell \in L$ then $\ell + L = 0 + L = 0 \in U$ and hence $\ell \in (U)$. In particular $0 \in (U)$. Next suppose we age given x, $y \in (U)$, that is $x + L$, $y + L \in U$. Then $(x + y) + L = (x + L) + (y + L) \in U$ as $U \leq_{\mathsf{m}} M/L$ and hence $x + y \in (U)$ again. Likewise for any $a \in R$ we get $(ax) + L = a(x + L) \in U$ and hence $ax \in (U)$, as $x + L \in U$ and $U \leq_{\mathsf{m}} M/L$. Thus both maps given are well-defined. It remains to verify that they are mutually inverse: the one direction is easy, consider any $U \leq_{\mathsf{m}} M/L$, then $U \mapsto (U) \mapsto (U)/L = \{ x + L \mid x + L \in U \} = U$. Conversely consider any $L \subseteq P \leq_{\mathsf{m}} M$, then $P \mapsto P/L \mapsto (P/L)$, yet using (i) we obtain $(P/L) = P$ from the following computation

$$\left(P \Big/ L\right) \;=\; \left\{ x \in M \mid x + L \in P \Big/ L \right\} \;=\; \{ x \in M \mid x \in P \} \;=\; P$$

(iii) To prove this claim we just have to iterate the equivalence in (i): $x + L \in (\bigcap_i P_i)/L$ is equivalent to $x \in \bigcap_i P_i$, which again is equivalent to $\forall\, i \in I : x \in P_i$. Now we use (i) once more to reformulate this into the equivalent statement $\forall\, i \in I : x + L \in P_i/L$, which obviously translates into $x + L \in \bigcap_i (P_i/L)$ again.

(iv) We want to verify $\sum_i (P_i/L) = (\sum_i P_i)/L$, to do this recall the explicit description of an arbitrary sum of sub-modules for the $P_i/L \leq_{\mathsf{m}} M/L$

$$\sum_{i \in I} \left(P_i \Big/ L\right) \;=\; \left\{ \sum_{i \in \Omega} (x_i + L) \;\middle|\; \Omega \subseteq I \text{ finite}, x_i + L \in P_i \Big/ L \right\}$$

Next recall the equivalence in (i), this allows us to simply substitute $x_i + L \in P_i/L$ by $x_i \in P_i$. Further - by definition of $+$ in M/L - we can rewrite the sum $\sum_i (x_i + L) = (\sum_i x_i) + L$. Together this yields

$$\sum_{i \in I} \left(P_i \Big/ L\right) \;=\; \left\{ \left(\sum_{i \in \Omega} x_i \right) + L \;\middle|\; \Omega \subseteq I \text{ finite}, x_i \in P_i \right\}$$

That is the term on the right hand side is (apart from the $+L$ in $(\sum_i x_i) + L$) nothing but the sum $\sum_i P_i$ again (by the explicit description of arbitrary sums of the sub-modules P_i. That is we have already arrived at our claim $\sum_i (P_i/L) = (\sum_i P_i)/L$.

(v) Let us denote $P_i' := P_i + L$, then it is clear that $L \subseteq P_i'$ for any $i \in I$. But on the other hand $\sum_i P_i' = \sum_i (P_i + L) = (\sum_i P_i) + L$ as the finitely many occurances of elements $\ell_i \in L$ can be composed to a single occurance of $\ell := \sum_i \ell_i \in L$. But by assumption L is already contained in $\sum_i P_i$ and hence $(\sum_i P_i) + L = \sum_i P_i$. That is we have obtained $\sum_i P_i' = \sum_i P_i$. Now statement (iv), that has just been proved, yields $(\sum_i P_i)/L = (\sum_i P_i')/L = \sum_i (P_i'/L)$, as claimed.

(vi) To prove this identity we directly refer to the definition of the R-sub-module generated by $X/L \subseteq M/L$. And this is given to be

$$\langle X/L \rangle_{\mathsf{m}} \;=\; \bigcap \Big\{ U \leq_{\mathsf{m}} M/L \;\Big|\; X/L \subseteq U \Big\}$$

By (ii) the sub-modules U of M/L correspond bijectively to the sub-modules P of M containing L. I.e. we may insert P/L for U, yielding

$$\langle X/L \rangle_{\mathsf{m}} \;=\; \bigcap \Big\{ P/L \;\Big|\; L \subseteq P \leq_{\mathsf{m}} M,\, X/L \subseteq P/L \Big\}$$

Clearly $X/L \subseteq P/L$ translates into $\forall\, x \in X : x + L \in P/L$, and due to the equivalence in (i) this is $\forall\, x \in X : x \in P$, i.e. $X \subseteq P$, therefore

$$\langle X/L \rangle_{\mathsf{m}} \;=\; \bigcap \Big\{ P/L \;\Big|\; L \subseteq P \leq_{\mathsf{m}} M,\, X \subseteq P \Big\}$$

Of course $L \subseteq P$ and $X \subseteq P$ can be written more compactly as $X \cap L \subseteq P$. And due to (iii) the intersection commutes with taking to quotients, such that we may reformulate

$$\langle X/L \rangle_{\mathsf{m}} \;=\; \bigcap \{ P \mid P \leq_{\mathsf{m}} M,\, X \cap L \subseteq P \} \big/ L$$

That is we have arrived at $\langle X/L \rangle_{\mathsf{m}} = \langle X \cup L \rangle_{\mathsf{m}}/L$. But by the explicit representation of the generated sub-modules (3.12) it is clear, that $\langle X \cap L \rangle_{\mathsf{m}} = \langle X \rangle_{\mathsf{m}} + \langle L \rangle_{\mathsf{m}}$. And as L already is a sub-module of M we have $\langle L \rangle_{\mathsf{m}} = L$. Altogether $\langle X/L \rangle_{\mathsf{m}} = (\langle X \rangle_{\mathsf{m}} + L)/L$.

□

Proof of (3.17):

- Let us first prove the identity part in the modular rule, starting with $(Q \cap U) + P \subseteq Q \cap (P + U)$. Thus we consider any $x \in Q \cap U$ and $p \in P$ and have to verify $x + p \in Q \cap (P + U)$. As $x \in Q$ and $p \in P \subseteq Q$ we have $x + p \in Q$. And as also $x \in U$ we have $x + p \in U + P$ hence the claim. Conversely for $(Q \cap U) + P \supseteq Q \cap (P + U)$ we are given any $p \in P$ and $u \in U$ such that $q := p + u \in Q$ and we have to verify $p + u \in (Q \cap U) + P$. But as $u = q - p$ and $p, q \in Q$ we find $u \in Q$ and hence $u \in Q \cap U$. And this already is $p + u = u + p \in (Q \cap U) + P$.

- So it remains to verify the implication in the modular rule. As $P \subseteq Q$ by assumption it remains to prove $Q \subseteq P$. Thus consider any $q \in Q$, then in particular $q \in Q + U = P + U$. That is there are $p \in P$ and $u \in U$ such that $q = p + u$. And as $p \in P \subseteq Q$ this yields $u = q - p \in Q$, such that $u \in Q \cap U = P \cap U$. In particular $u \in P$ and hence $q = p + u \in P$, as claimed.

□

Proof of (3.22):

(i) We will first prove that $\mathrm{ann}(X)$ is a left-ideal of R. As this is just the intersection of the annihilators $\mathrm{ann}(x)$ (where $x \in X$) it suffices to verify $\mathrm{ann}(x) \leq_{\mathsf{m}} R$ for any $x \in M$, due to (1.52). Now $0 \in \mathrm{ann}(x)$ is clear, as $0 \diamond x = 0$ for any $x \in M$. Now consider any two $a, b \in \mathrm{ann}(x)$, that is $ax = 0$ and $bx = 0$. Then $(a + b)x = (ax) + (bx) = 0 + 0 = 0$ and hence $a + b \in \mathrm{ann}(x)$ again.

Finally consider any $r \in R$, then $(ra)x = r(ax) = r \diamond 0 = 0$ and hence $ra \in \operatorname{ann}(x)$, as well. Altogether we have $\operatorname{ann}(x) \leq_{\mathsf{m}} R$ and hence $\operatorname{ann}(X) \leq_{\mathsf{m}} R$ is a left-ideal, as it is an intersection of such.

(i) Next we want to prove that $\operatorname{ann}(P) \trianglelefteq_{\mathsf{i}} R$ even is an ideal. As we already know $\operatorname{ann}(P) \leq_{\mathsf{m}} R$ it only remains to prove that $ar \in \operatorname{ann}(P)$ for any $a \in \operatorname{ann}(P)$ and any $r \in R$. As $a \in \operatorname{ann}(P)$ we have $ap = 0$ for any $p \in P$. Now consider any $x \in P$, then $rx \in P$, too as P is a sub-module of M. Thus $(ar)x = a(rx) = 0$, as we can take $p = rx$. And as $x \in P$ was arbitrary this means $ar \in \operatorname{ann}(P)$ again.

(ii) Let us denote $\Phi : R/\operatorname{ann}(x) \to Rx : \overline{b} := b + \operatorname{ann}(x) \mapsto bx$, we will first prove the well-definedness and injectivity of this map: $ax = \Phi(\overline{a}) = \Phi(\overline{b}) = bx$ is equivalent to $(a-b)x = 0$, that is $a - b \in \operatorname{ann}(x)$ or in other words $\overline{a} = a + \operatorname{ann}(x) = b + \operatorname{ann}(x) = \overline{b}$. The surjectivity of Φ is clear, as any $b \in R$ is allowed. And Φ also is a homomorphism of R-modules, as by definition of the algebraic operations of $R/\operatorname{ann}(x)$ we have $\Phi(\overline{a} + \overline{b}) = \Phi(\overline{a+b}) = (a+b)x = (ax) + (bx) = \Phi(\overline{a}) + \Phi(\overline{b})$ and $\Phi(a\overline{b}) = \Phi(\overline{ab}) = (ab)x = a(bx) = a\Phi(\overline{b})$. Nota that this proof was completely elementary. It can also be proved regarding the epimorphism $\varphi : R \to Rx : b \mapsto bx$ and noting that its kernel is $\operatorname{kn}(\varphi) = \operatorname{ann}(x)$. If we now invoke the first isomorphism theorem of R-modules, we get Φ.

(ii) If $\mathfrak{a} = \operatorname{ann}(x)$ for some $x \in M$ with $x \neq 0$, then we have just seen, that $\iota : R/\mathfrak{a} \xrightarrow{\sim} Rx \leq_{\mathsf{m}} M$ defined by $\iota(b + \mathfrak{a}) := bx$ is a monomorphism of the desired form. Conversely: As $\mathfrak{a}$ is proper we have $1 \notin \mathfrak{a}$ and thereby $1 + \mathfrak{a} \neq 0 \in R/\mathfrak{a}$. And as ι is injective, this means $x := \iota(1 + \mathfrak{a}) \neq 0 \in M$. Also for any $b \in R$ we have $\iota(b + \mathfrak{a}) = b\iota(1 + \mathfrak{a}) = bx$ such that $bx = 0$ is equivalent to $b + \mathfrak{a} = 0$ which again is $b \in \mathfrak{a}$. That is we have $\mathfrak{a} = \operatorname{ann}(x)$ for some $x \neq 0$.

(iii) First consider $x = 0$, then $ax = a0 = 0$ is clear for any $a \in S$ and hence $\operatorname{ann}(x) = S$. Secondly consider $x \neq 0$ and $a \in \operatorname{ann}(x)$, that is $ax = 0$. Suppose we had $a \neq 0$, too, then (as S is a skew-field) there was some $a^{-1} \in S$ such that $a^{-1}a = 1$. Then we would be able to compute $x = 1x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}0 = 0$, a contradiction to $x \neq 0$, such that $a = 0$ and therefore $\operatorname{ann}(x) = 0$. In other words $S \to Sx : a \mapsto ax$ is injective for any $x \neq 0$. But the surjectivity is trivial, so this map is an isomorhism of S-vector spaces.

(iv) Let us abbreviate $P := \langle X \rangle_{\mathsf{m}}$, then by definition it is clear that $X \subseteq P$ and hence $\operatorname{ann}(P) \subseteq \operatorname{ann}(X)$. For the converse inclusion consider any $a \in \operatorname{ann}(X)$, then we have to show $a \in \operatorname{ann}(P)$. That is $ap = 0$ for any $p \in P$. By (3.12) any $p \in P$ is given to be $p = \sum_i a_i x_i$ for some $a_i \in R$ and $x_i \in X$. Therefore $ap = \sum_i (aa_i)x_i = \sum_i a_i(ax_i) = \sum_i a_i 0 = 0$ as R is commutative. Altogether that is $\operatorname{ann}(X) = \operatorname{ann}(P)$. If X generates M, that is $P = M$, then we hence find $\operatorname{ann}(M) = \operatorname{ann}(X) = \bigcap_i \operatorname{ann}(x_i)$ as well.

(iv) Now suppose $M = \langle X \rangle_{\mathsf{m}}$ where $X = \{ x_i \mid i \in I \}$ and consider the map $\varphi : R \to M^I$ defined by $\varphi(a) := (ax_i)$ (where $i \in I$). If now $a \in \operatorname{ann}(M) = \operatorname{ann}(X)$ then $ax_i = 0$ for any $i \in I$ and hence $\varphi(a) = 0$ is clear. Therefore we have $\operatorname{ann}(M) \subseteq \operatorname{kn}(\varphi)$. Conversely $\varphi(a) = 0$ means $ax_i = 0$ for any $i \in I$, that is $a \in \operatorname{ann}(X) = \operatorname{ann}(M)$ and hence even $\operatorname{kn}(\varphi) = \operatorname{ann}(M)$. Thereby $R/\operatorname{ann}(M) \hookrightarrow M^I$ is well-defined and injective according to the first isomorphism theorem (3.78.(ii))

(v) We first have to check the well-definedness of the scalar multiplication. To do this consider any $b+\mathfrak{a} = c+\mathfrak{a}$, that is $a := c-b \in \mathfrak{a} \subseteq \operatorname{ann}_R(M)$. If now $x \in M$ is an arbitrary element, then $cx = (a+b)x = ax+bx = 0+bx = bx$, as a annihilates any $x \in M$. Hence $(b+\mathfrak{a}, x) \mapsto bx$ does not depend on the specific $b \in R$ chosen. As we have only changed the scalar-multiplication on M, it remains to prove, that it still satisfies the properties (M) in the definition of modules. Thus consider any $a, b \in R$ and any $x, y \in M$. Then we can compute

$$\begin{aligned}
(a+\mathfrak{a})(x+y) &= a(x+y) \;=\; ax+ay \\
&= (a+\mathfrak{a})x + (a+\mathfrak{a})y \\
((a+\mathfrak{a})+(b+\mathfrak{a}))x &= ((a+b)+\mathfrak{a})x \;=\; (a+b)x \\
&= ax+bx \;=\; (a+\mathfrak{a})x + (b+\mathfrak{a})x \\
((a+\mathfrak{a})(b+\mathfrak{a}))x &= ((ab)+\mathfrak{a})x \;=\; (ab)x \;=\; a(bx) \\
&= (a+\mathfrak{a})(bx) \;=\; (a+\mathfrak{a})((b+\mathfrak{a})x) \\
(1+\mathfrak{a})x &= 1x \;=\; x
\end{aligned}$$

□

Proof of (3.23):

(i) By definition an integral domain is non-zero $R \neq 0$, such that $1 \neq 0$. As also $1 \diamond 0 = 0$ we already have $0 \in \operatorname{tor}(M)$. Now consider any two $x, y \in \operatorname{tor}(M)$, that is there are some $0 \neq a, b \in R$ such that $ax = 0$ and $by = 0$. As R is an integral domain we also get $ab \neq 0$. Now compute $(ab)(x+y) = (ab)x + (ab)y = (ba)x + (ab)y = b(ax) + a(by) = b \diamond 0 + a \diamond 0 = 0+0 = 0$. That is $(ab)(x+y) = 0$ and hence $x+y \in M$, as $ab \neq 0$. Finally consider any $r \in M$, then we need to show $rx \in \operatorname{tor}(M)$. But this is clear from $a(rx) = (ar)x = (ra)x = r(ax) = r \diamond 0 = 0$.

(i) Let us abbreviate $T := \operatorname{tor}(M)$, now consider any $x+T \in \operatorname{tor}(M/T)$. That is there is some $0 \neq a \in R$ such that $(ax)+T = a(x+T) = 0+T$. This is just $ax \in T$, that is there is some $0 \neq b \in R$, such that $(ba)x = b(ax) = 0$. As R is an integral domain, we get $ba \neq 0$ and this means $x \in T$, such that $x+T = 0+T$. Thus we have just proved $\operatorname{tor}(M/T) \subseteq \{\, 0+T \,\} = \{0\}$ and the converse containment is clear.

(ii) Let $\{\, m_i \mid i \in I \,\}$ be a basis of M and consider any $x \in P$. Suppose there was some $0 \neq a \in R$ such that $ax = 0$. Then we write x as a linear combination of the m_i and find

$$x \;=\; \sum_{i \in I} x_i m_i \quad\Longrightarrow\quad 0 \;=\; ax \;=\; \sum_{i \in I} a x_i m_i$$

As the m_i are linearly independent, by assumption, this means $ax_i = 0$ for all $i \in I$. But as $a \neq 0$ and R is an integral domain this implies $x_i = 0$ for all $i \in I$ such that $x = 0$. That is we have proved that $ax = 0$ implies $x = 0$ for any $x \in P$. But this is $\operatorname{tor}(P) \subseteq 0$ and the converse inclusion is trivial.

(iii) (a) $\Longrightarrow$ (b): As $R \neq 0$ we have $1 \neq 0$ and as $1 \diamond 0 = 0$ this implies $0 \in \operatorname{tor}(M)$. Conversely consider any $x \in \operatorname{tor}(M)$, that is there is some $a \in R$ such that $a \neq 0$ but $ax = 0$. Suppose we had $x \neq 0$, then $a \in \operatorname{zd}_R(M) \subseteq \{0\}$ (by definition of $\operatorname{zd}_R(M)$, as $x \neq 0$ and $ax = 0$) which is

$a = 0$ again. But as $a \neq 0$ this is a contradiction. Thus we necessarily have $x = 0$ and as x has been arbitrary this means $\text{TOR}(M) \subseteq \{0\}$, as well.

(iii) (b) $\implies$ (c): Consider any $x \in M$ with $x \neq 0$, then $\text{ann}(x) = \{\, a \in R \mid ax = 0 \,\}$. If there was some $a \neq 0$ with $a \in \text{ann}(x)$, then $x \in \text{TOR}(M) = \{0\}$, which is untrue, as $x \neq 0$. Thus we have $\text{ann}(x) = 0$. As $M \neq 0$ we find (c).

(iii) (c) $\implies$ (d): Consider any $a \in R$ and any $x \in M$ such that $ax = 0$. If $x = 0$ we we are done, else $a \in \text{ann}(x) \in \text{Anns}(M) = \{0\}$. That is $a \in \text{ann}(x) = \{\, a \in R \mid ax = 0 \,\} = \{0\}$ and hence $a = 0$.

(iii) (d) $\implies$ (a): Consider any $a \in \text{ZD}_R(M)$, that is there is some $x \in M$ such that $x \neq 0$ and $ax = 0$. Thus by assumption (d) we find $a = 0$, and as a has been arbitrary, this means $\text{ZD}_R(M) \subseteq \{0\}$, as claimed.

(iv) (b) $\implies$ (a) is simple: If $\mu : M \hookrightarrow R^n$, then M is isomorphic to $N := \mu(M) \leq_{\mathsf{m}} R^n$. But as R^n is free [it has the Euclidean basis] and R is an integral domain (ii) tells us that N is torsion-free. Due to the isomorphism $\mu : M \xrightarrow{\sim} N$ this means M is torsion-free. Conversely for (a) $\implies$ (b) pick up a generating set $\{\, m_1, \ldots, m_r \,\}$ of M. If $M = 0$ we are done with $M \hookrightarrow R : 0 \mapsto 0$, so let us assume $M \neq 0$ and hence $m_i \neq 0$ for any $i \in 1 \ldots r$. Now let

$$\mathcal{L} \;:=\; \{\, I \subseteq 1 \ldots r \mid \{\, m_i \mid i \in I \,\} \text{ is linear independent} \,\}$$

By assumption $am_i \implies a = 0$ such that any $\{\, i \,\} \in \mathcal{L}$, in particular $\mathcal{L}$ is non-empty. But also $\mathcal{L}$ is finite [it contains 2^r elements at most]. So we may choose some $I \in \mathcal{L}$ that is maximal, that is $\{\, m_i \mid i \in I \,\}$ is linear independent and for any $j \notin I$ the set $\{\, m_i \mid i \in I \,\} \cup \{\, m_j \,\}$ is linearly dependent. Now let

$$\Phi \;:\; R^I \hookrightarrow M \;:\; (a_i) \mapsto \sum_{i \in I} a_i m_i$$

As $\{\, m_i \mid i \in I \,\}$ is linearly independent this homomorphism is injective. If we denote its image by $F := \text{im}(\Phi) \leq_{\mathsf{m}} M$ we even have an isomorphism $\Phi : R^I \xrightarrow{\sim} F \leq_{\mathsf{m}} M$. But by construction of I for any $j \in J$ the set $\{\, m_i \mid i \in I \,\} \cup \{\, m_j \,\}$ is linearly dependent, that is there are some $a_j \in R$ and some $a_{i,j} \in R$ (not all zero) such that

$$\sum_{i \in I} a_{i,j} m_i + a_j m_j \;=\; 0$$

If thereby $a_j = 0$, then there was some $a_{i,j} \neq 0$, which is absurd, since $\{\, m_i \mid i \in I \,\}$ is linear independent. But from this we get

$$a_j m_j \;=\; -\sum_{i \in I} a_{i,j} m_i \;\in\; \text{Lh}\{\, m_i \mid i \in I \,\} \;=\; F$$

If we take $a := \prod_{j \notin I} a_j$ then $a \neq 0$, as any $a_j \neq 0$ and R is an integral domain. But by construction also $am_j \in F$ for any $j \notin I$ and $am_i \in F$ for any $i \in I$ is clear. Thus we have $aM \subseteq F$. But as M is torsion free, the homomorphism

$$\alpha \;:\; M \hookrightarrow F \;:\; x \mapsto ax$$

has kernel $\mathrm{kn}(\alpha) = 0$, as $ax = 0$ implies $x = 0$. That means α is injective. And thereby we have found the embedding $\mu := \Phi^{-1}\alpha$ of M into R^I that is of the desired form

$$\Phi^{-1}\alpha \;:\; M \hookrightarrow F \;\xrightarrow{\sim}\; R^I$$

(v) If $x \in \mathrm{tor}(M)$ then there is some $0 \neq a \in R$ with $ax = 0$. But since Φ is a homomorphism this means $a\Phi(x) = \Phi(ax) = \Phi(0) = 0$ such that $\Phi(x) \in \mathrm{tor}(N)$. As x was arbitrary this means

$$\Phi(\mathrm{tor}(M)) \quad \subseteq \quad \mathrm{tor}(N)$$

With the same reasoning we find $\Phi^{-1}(\mathrm{tor}(N)) \subseteq \mathrm{tor}(M)$ and hence $\mathrm{tor}(N) \subseteq \Phi(\mathrm{tor}(M))$. Thus we have proved $\Phi(\mathrm{tor}(M)) = \mathrm{tor}(N)$. In particular $\Phi : \mathrm{tor}(M) \xrightarrow{\sim} \mathrm{tor}(N)$ is an isomorphism, as it is well-defined, surjective and inherits both the injectivity and the R-linearity from Φ. It remains to prove that

$$M\Big/_{\mathrm{tor}(M)} \;\xrightarrow{\sim}\; N\Big/_{\mathrm{tor}(N)} \;:\; x + \mathrm{tor}(M) \;\mapsto\; \Phi(x) + \mathrm{tor}(N)$$

is an isomorphism, as well. To do this regard $x + \mathrm{tor}(M) = y + \mathrm{tor}(M)$, that is $y - x \in \mathrm{tor}(M)$ and as Φ is injective this is equivalent to $\Phi(y - x) \in \Phi(\mathrm{tor}(M)) = \mathrm{tor}(N)$. As $\Phi(y - x) = \Phi(y) - \Phi(x)$ this is again equivalent to $\Phi(x) + \mathrm{tor}(N) = \Phi(y) + \mathrm{tor}(N)$. Thus we have established the well-definedness and injectivity at the same time. But as Φ is surjective so is $x + \mathrm{tor}(M) \mapsto \Phi(x) + \mathrm{tor}(N)$ and therefore we have another isomorphism.

(vi) Let us denote the set of all proper, pure sub-modules P of M by $\mathcal{P}$, that is $\mathcal{P} := \{ P \leq_{\mathfrak{m}} M \mid P \neq M, P \text{ is pure}$ As M is torsion free $0 \leq_{\mathfrak{m}} M$ is a pure sub-module of M ($ax = 0$ implies $a = 0$ or $x = 0$). Also $0 \neq M$ such that $\mathcal{P}$ is non-empty. Now consider a chain $(P_i) \subseteq \mathcal{P}$ in $\mathcal{P}$, then we let

$$Q \;:=\; \bigcup_{i \in I} P_i$$

As (P_i) is a chain we know that Q is a sub-module of M again. Now suppose we had $Q = M$. As M is finitely generated we find some $m_k \in M$ such that $M = \mathrm{Lh}(x_1, \ldots, x_n)$. And as (for any $k \in 1 \ldots n$) $x_k \in M = Q$ there is some $i(k) \in I$ such that $x_k \in P_{i(k)}$. Taking to the maximum of the $P_{i(k)}$ we find $x_k \in P_i$ for some $i \in I$. But this would imply $P_i = M$ in contradiction to our assumption. Hence $Q \neq M$.

In fact Q even is pure again: suppose we have $ax \in Q$, that is $ax \in P_i$ for some $i \in I$. And as this P_i has been pure we find $x \in P_i$ which yields $x \in Q$ again. Hence every chain (P_i) in $\mathcal{P}$ has an upper bound $Q \in \mathcal{P}$ and therefore $\mathcal{P}$ has a maximal element, due to the lemma of Zorn.

□

Proof of (3.24):

(i) Choose any $x \in M$, yet $x \neq 0$. Then $Rx = \{ bx \mid b \in R \}$ is a non-zero sub-module of M. But as $0 \neq Rx \leq_{\mathfrak{m}} M$ and M is simple we get $Rx = M$. Hence we get

$$\mathfrak{m} \;:=\; \mathrm{ann}_R(M) \;=\; \{ a \in R \mid \forall\, y \in Rx : ay = 0 \}$$

$$= \{ a \in R \mid \forall\, b \in R : abx = 0 \}$$
$$= \{ a \in R \mid ax = 0 \} = \operatorname{ann}(x)$$

Here $\{ a \in R \mid \forall\, b \in R : abx = 0 \} \subseteq \operatorname{ann}(x)$ is clear - just take $b = 1$. And the converse inclusion follows easily: if $ax = 0$, that $abx = b(ax) = b0 = 0$ as well. So by (ii) we obtain an isomorphy of R-modules

$$R\big/_{\mathfrak{m}} \xrightarrow{\sim} M \;:\; a + \mathfrak{m} \mapsto ax$$

Now, as M is simple, so is $R/\mathfrak{m}$. That is $0 = \mathfrak{m}/\mathfrak{m}$ is a maximal ideal of $R/\mathfrak{m}$. That is $R/\mathfrak{m}$ is a field and this again means that $\mathfrak{m}$ is a maximal ideal of R.

(ii) Let us first prove (b) $\Longrightarrow$ (a): That is we consider $ab \in \operatorname{ann}(x)$ and have to prove $a \in \operatorname{ann}(x)$ or $b \in \operatorname{ann}(x)$. Note that $ab \in \operatorname{ann}(x)$ is just $abx = 0$ and distinguish two cases: If $\operatorname{ann}(ax) = R$, then $1 \in \operatorname{ann}(ax)$ such that $ax = 0$, which is $a \in \operatorname{ann}(x)$. And if $\operatorname{ann}(ax) = \operatorname{ann}(x)$, then $bax = abx = 0$ can we put as $b \in \operatorname{ann}(ax) = \operatorname{ann}(x)$, such that $b \in \operatorname{ann}(x)$. Altogether $\operatorname{ann}(x)$ is prime.

It remains to prove (a) $\Longrightarrow$ (b): Clearly, if $a \in \operatorname{ann}(x)$, then $ax = 0$ such that $\operatorname{ann}(ax) = \operatorname{ann}(0) = R$. So let us assume $a \notin \operatorname{ann}(x)$ and consider $b \in \operatorname{ann}(ax)$. That is $bax = 0$ and hence $ba \in \operatorname{ann}(x)$. As $\operatorname{ann}(x)$ is prime and $a \notin \operatorname{ann}(x)$ this implies $b \in \operatorname{ann}(x)$. Thus we have proved $\operatorname{ann}(ax) \subseteq \operatorname{ann}(x)$. But the converse inclusion $\operatorname{ann}(x) \subseteq \operatorname{ann}(ax)$ is generally true: if $b \in \operatorname{ann}(x)$ then $bx = 0$, in particular $0 = a\,0 = a\,bx = b\,ax$ such that $b \in \operatorname{ann}(ax)$, as well. Thus we have $\operatorname{ann}(x) = \operatorname{ann}(ax)$ in case $a \notin \operatorname{ann}(x)$.

(iii) By definition $\operatorname{Anns}(Ry)$ is the set of all $\operatorname{ann}(z)$ for some $z \in Ry$ with $z \neq 0$. As $a \notin \mathfrak{p} = \operatorname{ann}(x)$ we have $y = ax \neq 0$ and as $y \in Ry$ this is $\operatorname{ann}(y) \in \operatorname{Anns}(Ry)$ such that $\operatorname{Anns}(Ry) \neq \emptyset$. It remains to verify, that $\operatorname{ann}(by) = \mathfrak{p}$ for any $b \in R$ such that $by \neq 0$. As $y = ax$ this is $\operatorname{ann}(bax) = \mathfrak{p} = \operatorname{ann}(x)$ whenever $bax \neq 0$. As $bax \neq 0$ we also have $ax \neq 0$. Then $b \notin \operatorname{ann}(ax)$ implies $\operatorname{ann}(ax) \neq 0$ and as $\operatorname{ann}(x)$ is prime, (ii) only leaves the option $\operatorname{ann}(ax) = \operatorname{ann}(x)$. But also $\operatorname{ann}(bax) =\neq R$ (as $1 \notin \operatorname{ann}(abx)$) and $\operatorname{ann}(ax) = \operatorname{ann}(x)$ is prime, such that (ii) implies $\operatorname{ann}(by) = \operatorname{ann}(bax) = \operatorname{ann}(x) = \mathfrak{p}$ again.

(iii) Let $\mathfrak{p} = \operatorname{ann}(x)$ be a maximal annihilator ideal of M with $\mathfrak{p} \neq R$. Further consider any $a, b \in R$ with $ab \in \mathfrak{p}$ but $b \notin \mathfrak{p}$, then it remains to verify $a \in \mathfrak{p}$. As $b \notin \mathfrak{p}$ we have $bx \neq 0$. Now consider $\mathfrak{a} := \operatorname{ann}(bx)$, as $bx \neq 0$ we have $1 \notin \mathfrak{a}$ and hence $\mathfrak{a} \neq R$. Also if $p \in \mathfrak{p}$, then $p(bx) = b(px) = b0 = 0$ and hence $p \in \mathfrak{a}$, which means $\mathfrak{p} \subseteq \mathfrak{a}$. But by maximality of $\mathfrak{p}$ this is $\mathfrak{p} = \mathfrak{a}$. Now as $ab \in \mathfrak{p}$ we have $a(bx) = (ab)x = 0$ such that $a \in \mathfrak{a} = \mathfrak{p}$, as has been claimed.

□

Proof of (3.25):
Let us first prove that $Q : P$ is a sub-module of R: As $0\,P = 0 \subseteq Q$ we always have $0 \in Q : P$. Now if a, $b \in Q : P$ then for any $p \in P$ we get $ap \in aP \subseteq Q$ and $bp \in bP \subseteq Q$ such that $(a+b)p = ap + bp \in Q$, as Q is a sub-module of M, and hence $a + b \in Q : P$. And if $a \in Q : P$ then $aP \subseteq Q$, such that for any $b \in R$ we find $(ba)P = b(aP) \subseteq bQ \subseteq Q$ and hence $ba \in Q : P$ again. Together this is $Q : P \leq_{\mathsf{m}} R$. And $0 : M = \{ a \in R \mid aM \subseteq 0 \} = \operatorname{ann}(M)$ is obvious.
If now R is commutative, then $Q : P \leq_{\mathsf{m}} R$ implies $Q : P \trianglelefteq_{\mathsf{i}} R$ and we look at $\operatorname{ann}(x) = \{ a \in R \mid ax = 0 \}$ and $0 : Rx = \{ a \in R \mid aRx \subseteq 0 \}$. As $x \in Rx$ we get $a \in 0 : Rx \Longrightarrow a \in \operatorname{ann}(x)$. Conversely as R is

commutative $ax = 0$ implies $a(bx) = b(ax) = b\,0 = 0$ for any $b \in R$ such that $a \in 0 : Rx$, as well. □

Proof of (3.29):

- We will first verify that the exterior direct product $P := \prod_i M_i$ is an R-module again (under the operations given). The well-definedness of the operations is clear. Thus consider $x = (x_i)$, $y = (y_i)$ and $z = (z_i) \in P$. Then $x + (y + z) = (x_i + (y_i + z_i)) = ((x_i + y_i) + z_i) = (x + y) + z$ which is the associativity. Likewise $x + y = (x_i + y_i) = (y_i + x_i) = y + x$, which is the commutativity. Letting $0 := (0_i)$, where $0_i \in M_i$ is the zero-element, we find $x + 0 = (x_i + 0_i) = (x_i) = x$, such that $0 \in P$ is the zero-element. And the negative of x is $\overline{x} = (-x_i) \in P$, as $x + \overline{x} = (x_i + (-x_i)) = (0_i) = 0$. Now consider any a, $b \in R$ then $a(x + y) = (a(x_i + y_i)) = ((ax_i) + (ay_i)) = (ax_i) + (ay_i) = (ax) + (ay)$. Likewise $(a + b)x = ((a + b)x_i) = ((ax_i) + (bx_i)) = (ax_i) + (bx_i) = (ax) + (bx)$ and $(ab)x = ((ab)x_i) = (a(bx_i)) = a(bx_i) = a(bx)$. Finally $1x = (1x_i) = (x_i) = x$, such that altogether P is an R-module again.

- Let us now verify that the direct sum $S := \bigoplus_i M_i$ is an R-sub-module of the direct product P. Thus we only have to prove that S is closed under the operations of P. However for any $a \in R$ and any x, $y \in S$ it is clear that $\mathrm{Supp}(ax) \subseteq \mathrm{Supp}(x)$ and $\mathrm{Supp}(x + y) \subseteq \mathrm{Supp}(x) \cup \mathrm{Supp}(y)$. Hence $\#\mathrm{Supp}(ax) \leq \#\mathrm{Supp}(x) < \infty$ and $\#\mathrm{Supp}(x + y) \leq \#\mathrm{Supp}(x) + \#\mathrm{Supp}(y) < \infty$. Thereby ax and $x + y \in S$ again.

- If now A_i is an R-semi-algebra (where $i \in I$ again) then we have verified that $P = \prod_i A_i$ is an R-module already. So let us again consider $x = (x_i)$, $y = (y_i)$ and $z = (z_i) \in A$ again. Then $x(yz) = (x_i)(y_i z_i) = (x_i(y_i z_i)) = ((x_i y_i)z_i) = (x_i y_i)(z_i) = (xy)z$ and likewise $x(y + z) = (x_i)(y_i + z_i) = (x_i(y_i + z_i)) = (x_i y_i + x_i z_i) = (x_i y_i) + (x_i z_i) = xy + xz$ and $(x + y)z = (x_i + y_i)(z_i) = ((x_i + y_i)z_i) = (x_i z_i + y_i z_i) = (x_i z_i) + (y_i z_i) = xz + yz$. Also for any $a \in R$ we get $a(xy) = a(x_i y_i) = (a(x_i y_i)) = ((ax_i)y_i) = (ax_i)(y_i) = (ax)y$ and likewise $a(xy) = a(x_i y_i) = (a(x_i y_i)) = (x_i(ay_i)) = (x_i)(ay_i) = x(ay)$. Altogether A is an R-semi-algebra again. And as clearly $\mathrm{Supp}(xy) \subseteq \mathrm{Supp}(x) \cap \mathrm{Supp}(y)$ we get $xy \in S := \oplus_i A_i$ in case x and $y \in S$. Hence S is an R-sub-semi-algebra of P.

 Now suppose any A_i even is an R-algebra featuring the unit element 1_i. Then for any $x = (x_i) \in P$ we get $(1_i)x = (1_i)(x_i) = (1_i x_i) = (x_i) = x$ and $x(1_i) = (x_i)(1_i) = (x_i 1_i) = (x_i) = x$. That is (1_i) is the unit element of P again, such that P is an R-algebra, as well. Note however, that if $A_i \neq 0$ for infinitely many $i \in I$, then S is *not* an R-algebra, as $1 = (1_i) \in P \setminus S$ will not be contained in S.

- Now consider the R-module-homomorphisms $\varphi_i : M_i \to N$. By construction of S the map $\varphi := \bigoplus_i \varphi_i : S \to N$ is well-defined. And it also is an R-module-homomorphism, as for any $a \in R$ and for any $x = (x_i)$, $y = (y_i) \in S$ we get $\varphi(ax) = \sum_i \varphi_i(ax_i) = \sum_i a\varphi_i(x_i) = a\varphi(x)$ and $\varphi(x + y) = \sum_i \varphi_i(x_i + y_i) = \sum_i (\varphi_i(x_i) + \varphi_i(y_i)) = \varphi(x) + \varphi(y)$.

- (a) $\Longrightarrow$ (b): by definition of the arbitrary sum of the sub-modules P_i of M and by the assumption $M = \sum_i P_i$ we obtain the identity

$$M \;=\; \left\{ \sum_{i \in \Omega} x_i \;\middle|\; \Omega \subseteq I \text{ finite}, x_i \in P_i \right\}$$

Thus if we are given any $x \in M$ there are finitely many $x_i \in P_i$ ($i \in \Omega$) such that $x = \sum_i x_i$ Letting $x_i := 0$ for $i \in I \setminus \Omega$ we obtain an extension $(x_i) \in \bigoplus_i P_i$ satisfying $x = \sum_i x_i$. This proves the existence of such a representation. For the uniqueness suppose $\sum_i x_i = \sum_i y_i$ for some (x_i), $(y_i) \in \bigoplus_i P_i$. Fix any $j \in I$ and let

$$\widehat{x}_j := \sum_{i \neq j} x_i \quad \text{and} \quad \widehat{y}_j := \sum_{i \neq j} y_i \quad \in \quad \widehat{P}_j$$

Then we find $x_j - y_j = \widehat{y}_j - \widehat{x}_j$, but as $x_j - y_j \in P_j$ and $\widehat{y}_j - \widehat{x}_j \in \widehat{P}_j$ we have $x_j - y_j \in P_j \cap \widehat{P}_j = 0$, such that $x_j = y_j$. But as $j \in I$ has been arbitrary this means $(x_i) = (y_i)$, which also is the uniqueness.

- (b) $\implies$ (a): consider any $x \in M$, by asumption (b) there is some $(x_i) \in \bigoplus_i P_i$ such that $x = \sum_i x_i$. And as only finitely many x_i are non-zero this means $x = \sum_i x_i \in \sum_i P_i$. And as x has been arbitrary this already is $M = \sum_i P_i$. Now consider any $j \in I$ and any $x \in P_j \cap \widehat{P}_j$. As $x \in P_j$ we may let $\widetilde{x}_j := x_j \in P_j$ and $\widetilde{x}_i := 0 \in P_i$ (for $i \neq j$) to find $x = \sum_i \widetilde{x}_i$. On the other hand we have $x \in \widehat{P}_j$, that is there are some $x_i \in P_i$ such that $x = \sum_{i \neq j} x_i$. Finally let $x_j := 0$ then altogether this is $\sum_i x_i = \sum_{i \neq j} x_i = \sum_i \widetilde{x}_i$ and due to the uniqueness this means $x_i = \widetilde{x}_i$ for any $i \in I$. But by choice of $\widetilde{x}_i$ this is $x_i = 0$ for any $i \neq j$ and hence $x = \sum_{i \neq j} 0 = 0$, which had to be shown.

□

Proof of (3.30):
Let us again abbreviate the exterior direct product by $P := \prod_i M_i$ and the exterior direct sum by $S := \bigoplus_i M_i$. It is immediately clear that $\pi_j : P \to M_j$ is an R-module-homomorphism: $\pi_j(ax + y) = \pi_j((ax_i + y_i)) = ax_j + y_j = a\pi_j(x) + \pi_j(y)$ Analogously it is clear that ι_j is an R-module homomorphism. Also $\pi_j \iota_j(x_j) = \pi_j(\delta_{i,j} x_j) = \delta_{j,j} x_j = x_j$ such that $\pi_j \iota_j = \mathbb{1}$. And from this it immediately follows that π_j is surjective and that π_j is injective. Note that the latter could have also been seen directly. Now consider any $x = (x_i) \in P$, then by definition $\pi_i(x) = x_i$ such that $x = (x_i) = (\pi_i(x))$. Conversely consider $x = (x_i) \in S$, then by definition $\iota_j(x_j) = (\delta_{i,j} x_j)$ (where the index runs over all $i \in I$). Therefore a straightforard computation yields

$$\sum_{j \in I} \iota_j(x_j) \quad = \quad \sum_{j \in I} \Big(\delta_{i,j} x_j \Big) \quad = \quad \left(\sum_{j \in I} \delta_{i,j} x_j \right) \quad = \quad (x_i) \quad = \quad x$$

□

Proof of (3.34):

(i) It is easy to see that the map given is a homomorphism: $(x_i) + (y_i) = (x_i + y_i) \mapsto \sum_i (x_i + y_i) = (\sum_i x_i) + (\sum_i y_i)$ and $a(x_i) = (ax_i) \mapsto \sum_i (ax_i) = a(\sum_i x_i)$. And the bijectivity is just a reformulation of property (b) of inner direct sums.

(ii) Let us abbreviate the exterior direct sum by $M := \bigoplus_i M_i$. That is any $x \in M$ is of the form $x = (x_i)$ for some $x_i \in M_i$ of which only finitely many are non-zero. Thus $x = (x_i) = \sum_i \iota_i(x_i) \in \sum_i P_i$. And as x has been arbitrary this means $M = \sum_i P_i$. Now consider any $j \in I$ and any $x \in P_j \cap \widehat{P}_j$. As $x \in P_j = \iota_j(M_j)$ there is some $m_j \in M_j$ such that $(x_i) := x = \iota_j(m_j) = (\delta_{i,j} m_j)$. On the other hand there are $p_i \in P_i$ (where $i \neq j$) such that $x = \sum_{i \neq j} p_i$. Likewise we choose $n_i \in M_i$ such that

$p_i = \iota_i(n_i)$. If we finally let $n_j := 0$, then $x = \sum_{i\neq j} \iota_i(n_i) = \sum_i \iota_i(n_i) = (n_i)$. Comparing these two expressions of x we find $n_i = x_i = \delta_{i,j} m_j = 0$ for any $i \neq j$. And as also $n_j = 0$ this means $x = (n_i) = (0_i) = 0 \in M$. Therefore $P_j \cap \widehat{P}_j = 0$, as claimed.

□

Proof of (3.35):
First of all note that $P_i \leq_{\mathsf{m}} M_i$ and $M_i \leq_{\mathsf{m}} M$ implies $P_i \leq_{\mathsf{m}} M$, that is the P_i are sub-modules of M. And thereby their sum P is a sub-module of M, as well. We now prove that this sum even is direct: For this it suffices to show, that for any $j \in I$ we have

$$P_j \cap \widehat{P}_j \;=\; 0$$

But clearly $P_j \subseteq M_j$ and likewise $\widehat{P}_j \subseteq \widehat{M}_j$ and as M was assumed to be a direct sum of the M_i this implies $P_j \cap \widehat{P}_j \subseteq M_j \cap \widehat{M}_j = 0$, such that P is an inner direct sum of the P_i as well.
It remains to verify that $\Phi(x_i + P_i) = \sum_i x_i + P$ truly is a well-defined isomorphism of R-modules. First of all note, that all the sums in question always are finite, as we are speaking of direct sums only. Thus it makes sense to write $\sum_i x_i$ even if I is infinite. For the well-definedness we need to regard two sequences $(x_i + P_i) = (y_i + P_j)$, that is for any $i \in I$ we have $p_i := y_i - x_i \in P_i$. Thereby $\sum_i p_i \in P$ such that $\sum_i y_i - \sum_i x_i \in P$. But this again is $\sum_i x_i + P = \sum_i y_i + P$, as needed.
The surjectivity of Φ is straightforward: Given any $x \in M$ there are some $x_i \in M_i$ (where $i \in I$) such that $x = \sum_i x_i$. Then in particular we find

$$\Phi\big(x_i + P_i\big) \;=\; \left(\sum_{i\in I} x_i\right) + P \;=\; x + P$$

For the injectivity we consider $\sum_i x_i + P = \sum_i y_i + P$ or in other words $\sum_i (y_i - x_i) \in P$. Hereby $y_i - x_i \in M_i$ for any $i \in I$. Let us now denote the canonical projection (where $j \in I$)

$$\pi_j \;:\; M \;\to\; M_j \;:\; \sum_{i\in I} x_i \;\mapsto\; x_j$$

This is well-defined, since the x_i in the sum $\sum_i x_i \in M$ are uniquely determined (as M is an inner direct sum of the M_i). We now prove, that

$$\pi_j(P) \;=\; P_j$$

Clearly any $p_j \in P_j \subseteq M_j$ satifsies $\pi_j(p_j) = p_j$ such that $p_j \in \pi_j(P)$. Conversely, if $p \in P$ then by construction of P there are some $p_i \in P_i$ such that $p = \sum_i p_i$. Thereby $p_i \in P_i \subseteq M_i$ such that $\pi_j(p) = p_j \in P_j$. Thus we have proved $\pi_j(P) = P_j$. Once this is out of the way we apply π_j to $\sum_i (y_i - x_i) \in P$. As $y_i - x_i \in M_i$ we get

$$y_j - x_j \;=\; \pi_j\left(\sum_{i\in I} (y_i - x_i)\right) \;\in\; \pi_j(P) \;=\; P_j$$

and this is $y_j + P_j = x_j + P_j$. As $j \in I$ has been arbitrary we find that the entire sequences $(x_i + P_i) = (y_i + P_i)$ are equal, which means that Φ also is injective. Altogether Φ is an isomorphism. □

Proof of (3.37):

- Clearly the map $\varphi \mapsto (\pi_j \varphi \iota_i)$ is well-defined: as π_j and ι_i are R-module homomorphisms, so is the composition $\pi_j \varphi \iota_i : M_i \to N_j$. Conversely $(\varphi_{i,j}) \mapsto (\bigoplus_i \varphi_{i,j})$ is well-defined, too - it just is the cartesian product of the induced homomorphisms $\bigoplus_i \varphi_{i,j} : \bigoplus_i M_i \to N_j$.

- And it is also clear, that $\varphi \mapsto (\pi_j \varphi \iota_i)$ is a homomorphism of R-modules: as ι_i and π_j are homomorphisms of R-modules, so are the push-forward $\varphi \mapsto \varphi \iota_i$ and pull-back $\psi \mapsto \pi_j \psi$. Combining these we see that $\varphi \mapsto \pi_j \varphi \iota_i$ is a homomorphism of R-modules. Thus if we regard any $\varphi, \psi \in \mathrm{mhom}(M, N)$ and any $a \in R$, then $a\varphi + \psi \mapsto (\pi_j(a\varphi + \psi)\iota_i) = (a\pi_j \varphi \iota_i + \pi_j \psi \iota_i) = a(\pi_j \varphi \iota_i) + (\pi_j \psi \iota_i)$, as the composition in the direct product was defined to be component-wise.

- We will now prove that these maps are mutually inverse, we start by regarding $\varphi \mapsto (\pi_j \varphi \iota_i) \mapsto \psi := (\bigoplus_i \pi_j \varphi \iota_i)$. Thus consider an arbitrary $x = (x_i) \in \bigoplus_i M_i$ then we find

$$\psi(x) \;=\; \left(\sum_{i \in I} \pi_j \varphi \iota_i(x_i) \right) \;=\; \left(\pi_j \varphi \left(\sum_{i \in I} \iota_i(x_i) \right) \right)$$

 as $\pi_j \varphi$ is an R-module homomorphism. Now recall the identities $x = \sum_i \iota_i(x_i)$ and $y = (\pi_j(y))$, inserting these we obtain $\psi = \varphi$ from

$$\psi(x) \;=\; \Big(\pi_j \varphi(x) \Big) \;=\; \varphi(x)$$

- Thus we have to regard $(\varphi_{i,j}) \mapsto (\bigoplus_i \varphi_{i,j}) \mapsto (\psi_{i,j}) := (\pi_j(\bigoplus_i \varphi_{i,j})\iota_i)$. We need to verify that for any $i \in I$ and $j \in J$ we get $\varphi_{i,j} = \psi_{i,j}$. Thus fix any i, j and $x_i \in M_i$ and compute

$$\psi_{i,j}(x_i) \;=\; \pi_j \left(\left(\bigoplus_{a \in I} \varphi_{a,b} \right)_{b \in J} \Big(\iota_i(x_i) \Big) \right)$$

 By definition we have $\iota_i(x_i) = (\delta_{a,i} x_i)$, where the index runs over $a \in I$. Inserting this into the definition of $\bigoplus_a \varphi_{a,b}$ we continue

$$\psi_{i,j}(x_i) \;=\; \pi_j \left(\sum_{a \in I} \varphi_{a,b}(\delta_{a,i} x_i) \right)_{b \in J} \;=\; \sum_{a \in I} \varphi_{a,j}(\delta_{a,i} x_i)$$

 If $a \neq i$ then $\delta_{a,i} x_i = 0 \in M_a$ such that the respective summand vanishes. It only remains the summand of $a = i$, which is given to be $\varphi_{i,j}(\delta_{i,i} x_i) = \varphi_{i,j}(x_i)$. As x_i has been arbitrary this proves $\psi_{i,j} = \varphi_{i,j}$ which had to be shown.

- We now prove the claim in the remark to the proposition: that is we consider $\varphi_i := (\varphi_{i,j}) \in \bigoplus_j \mathrm{mhom}(M_i, N_j)$ and want to show that the image of the corresponding map $\varphi := (\bigoplus_i \varphi_{i,j})$ is contained in $\bigoplus_j N_j$. Thus consider any $x = (x_i) \in \bigoplus_i M_i$ then we have to verify, that

$$y \;:=\; \varphi(x) \;=\; \left(\sum_{i \in I} \varphi_{i,j}(x_i) \right) \;\in\; \bigoplus_{j \in J} N_j$$

 That is we have to verify that the support of y is finite. To see this let us abbreviate the support of x by $\Omega := \mathrm{Supp}(x) \subseteq I$, which is a finite set, as $x \in \bigoplus_i M_i$. Then it is clear that the support of

y satisfies the following inclusions

$$\begin{aligned}
\mathrm{Supp}(y) &= \left\{ j \in J \;\middle|\; \sum_{i\in I} \varphi_{i,j}(x_i) \neq 0 \right\} \\
&\subseteq \left\{ j \in J \mid \exists\, i \in I \;:\; \varphi_{i,j}(x_i) \neq 0 \right\} \\
&\subseteq \left\{ j \in J \mid \exists\, i \in I \;:\; x_i \neq 0 \text{ and } \varphi_{i,j} \neq 0 \right\} \\
&= \left\{ j \in J \mid \exists\, i \in \Omega \text{ with } \varphi_{i,j} \neq 0 \right\} \\
&= \bigcup \{\, \mathrm{Supp}(\varphi_i) \mid i \in \Omega \,\}
\end{aligned}$$

However the latter is a finite (Ω is finite) union of finite (any $\mathrm{Supp}(\varphi_i)$ was assumed to be finite) subsets of J. Hence it is a finite set itself which proves $y \in \bigoplus_j N_j$ which had been claimed.

□

Proof of (3.40):

(i) Recall that $\mathfrak{a}P$ has been defined to be the sub-module generated by elements of the form αp with $\alpha \in \mathfrak{a}$ and $p \in P$. In the light of (3.12) this turns into

$$\begin{aligned}
\mathfrak{a}P &= \mathrm{Lh}\{\, \alpha p \mid \alpha \in \mathfrak{a},\ p \in P \,\} \\
&= \left\{ \sum_{i=1}^{n} b_i \alpha_i p_i \;\middle|\; 1 \leq n \in \mathbb{N},\ b_i \in R,\ \alpha_i \in \mathfrak{a},\ p_i \in P \right\}
\end{aligned}$$

But as $\mathfrak{a}$ is an ideal and $\alpha_i \in \mathfrak{a}$ we find that $a_i := b_i\alpha_i \in \mathfrak{a}$ again. And hence $\mathfrak{a}P$ is contained in the set given in claim (i). Conversely any $a_1p_1 + \cdots + a_np_n$ can be realized by taking $b_1 = \cdots = b_n = 1$ and $\alpha_i = a_i$. Thus the set given in claim (i) is also contained in $\mathfrak{a}P$:

$$\mathfrak{a}P = \left\{ \sum_{i=1}^{n} a_i p_i \;\middle|\; 1 \leq n \in \mathbb{N},\ a_i \in \mathfrak{a},\ p_i \in P \right\}$$

(ii) As $x \in \mathfrak{a}P$ there are some $\alpha_1, \ldots, \alpha_m \in \mathfrak{a}$ and $q_1, \ldots, q_m \in P$ such that $x = \alpha_1q_1 + \cdots + \alpha_mq_m$ as we have seen in (i). In the first case let P be generated by $\{\, p_j \mid j \in J \,\}$, then the elements q_k can be written in the following form

$$q_k = \sum_{j\in J} b_{k,j} p_j$$

for some $b_{k,j} \in R$, of which only finitely many are non-zero. That is for any $k \in 1 \ldots m$ the set $J(k) := \{\, j \in J \mid b_{k,j} \neq 0 \,\}$ is finite. Inserting these equations into our presentation of x we find

$$x = \sum_{k=1}^{m} \alpha_k q_k = \sum_{k=1}^{m} \alpha_k \left(\sum_{j\in J} b_{k,j} p_j \right) = \sum_{j\in J} \left(\sum_{k=1}^{m} \alpha_k b_{k,j} \right) p_j$$

If $j \notin J(1) \cup \cdots \cup J(m)$ then $b_{k,j} = 0$ for any $k \in 1 \ldots m$. In this case the element $a_j := \sum_k \alpha_k b_{k,j}$ is zero and hence the sum is well-defined, as it only runs over the finite set $J(1) \cup \cdots \cup J(m)$. Also, as $\mathfrak{a}$ is an ideal all the elements a_j(for any $j \in J$) are contained in $\mathfrak{a}$ again. Let us denote the non-zero $a_j \in \mathfrak{a}$ by $a_1, \ldots, a_n$ and the corresponding p_j by $p_1, \ldots, p_n$, then we have arrived at the first claim $x = a_1p_1 + \cdots + a_np_n$.

In the second case R is commutative and we assume that $\mathfrak{a}$ is generated by the set $\{ a_i \mid i \in I \}$. Then any scalar α_k can be written in the following form

$$\alpha_k \;=\; \sum_{i\in I} b_{k,i}a_i$$

for some $b_{k,i} \in R$, of which only finitely many are non-zero. That is for any $k \in 1\ldots m$ the set $I(k) := \{ i \in I \mid b_{k,i} \neq 0 \}$ is finite. Inserting these equations into our presentation of x we find

$$x \;=\; \sum_{k=1}^{m} \alpha_k q_k \;=\; \sum_{k=1}^{m} \left(\sum_{i\in I} b_{k,i}a_i \right) q_k \;=\; \sum_{i\in I} a_i \left(\sum_{k=1}^{m} b_{k,i}q_k \right)$$

If $i \notin I(1) \cup \cdots \cup I(m)$ then $b_{k,i} = 0$ for any $k \in 1\ldots m$. In this case the element $p_i := \sum_k b_{k,i}q_k$ is zero and hence the sum is well-defined, as it only runs over the finite set $I(1) \cup \cdots \cup I(m)$. Also, as P is a sub-module all the elements p_i are contained in P again. Let us denote the non-zero $p_i \in P$ by $p_1, \ldots, p_n$ and the corresponding a_i by $a_1, \ldots, a_n$, then we have arrived at the second claim $x = a_1p_1 + \cdots + a_np_n$.

(iii) As $ap \in P$ for any $a \in \mathfrak{a} \subseteq R$ and any $p \in P$, so is the sub-module generated by these elements - and this is $\mathfrak{a}P$.

(iv) Considering the ideals $\mathfrak{a}$ and $\mathfrak{b}$ with $\mathfrak{a} \subseteq \mathfrak{b}$ we find that for any $a \in \mathfrak{a} \subseteq \mathfrak{b}$ and any $p \in P$ we get $ap \in \mathfrak{a}P$ and hence $\mathfrak{a}P \subseteq \mathfrak{b}P$. In complete analogy: Considering the submdules P and Q with $P \subseteq Q$ we find that for any $a \in \mathfrak{a}$ and any $p \in P \subseteq Q$ we get $ap \in \mathfrak{a}Q$ and hence $\mathfrak{a}P \subseteq \mathfrak{a}Q$.

(v) We first prove that $\mathfrak{a}(M/P)$ is contained in $(\mathfrak{a}M + P)/P$, to do this, consider any element of $\mathfrak{a}(M/P)$, by definition this is of the form (where $a_k \in \mathfrak{a}$ and $x_k \in M$)

$$\sum_{k=1}^{n} a_k(x_k + P) \;=\; \left(\sum_{k=1}^{n} a_k x_k \right) + P \;\in\; \mathfrak{a}M + P \Big/ P$$

That is $\mathfrak{a}(M/P) \subseteq (\mathfrak{a}M + P)/P$, conversely consider any element of $\mathfrak{a}M + P$, that is we are given any $a_k \in \mathfrak{a}$, $x_k \in M$ and $p \in P$, then

$$\begin{aligned} \left(\sum_{k=1}^{n} a_k x_k \right) + p + P \;&=\; \left(\sum_{k=1}^{n} a_k x_k \right) + P \\ &=\; \sum_{k=1}^{n} a_k(x_k + P) \;\in\; \mathfrak{a}\left(M \Big/ P \right) \end{aligned}$$

That is $(\mathfrak{a}M + P)/P \subseteq \mathfrak{a}(M/P)$ as well and hence we have proved the equality of these sets, which had been claimed.

(vi) By definition (3.14) of the quotient module $M/\mathfrak{a}M$ is a well-defined R-module. Hence all we have to do is checking the well-definedness of the scalar-multiplication. We will present two ways of demonstrating this: (1) clearly we get $a(x + \mathfrak{a}M) = ax + \mathfrak{a}M = 0 + \mathfrak{a}M$ for any $a \in \mathfrak{a}$ and any $x \in M$. That is $\mathfrak{a} \subseteq \operatorname{ann}_R(M/\mathfrak{a}M)$, such that we could simply cite (3.22.(v)). The more instructive way (2) is a direct computation however: consider $b + \mathfrak{a} = c + \mathfrak{a}$ and $x + \mathfrak{a}M = y + \mathfrak{a}M$, that is

$a := c - b \in \mathfrak{a}$ and $p := y - x \in \mathfrak{a}M$. Then $cy - bx = cy - by + by - bx = (c-b)y + b(y-x) = ay + bp$. But as $a \in \mathfrak{a}$ we find that $ay \in \mathfrak{a}M$ and as $p \in \mathfrak{a}M$ already we see that $cy - bx \in \mathfrak{a}M$. But this is $bx + \mathfrak{a}M = cy + \mathfrak{a}M$ and hence $(b + \mathfrak{a}, x + \mathfrak{a}M) \mapsto bx + \mathfrak{a}M$ does not depend on the specific choice of $b \in R$ or $x \in M$.

(vii) We first have to check the well-definedness of $\varphi/\mathfrak{a}$: to do this we consider any $x + \mathfrak{a}M = y + \mathfrak{a}M$ in $M/\mathfrak{a}M$, that is $p := y - x \in \mathfrak{a}M$. By definition of $\mathfrak{a}M$ this means that p can be written as $p = a_1p_1 + \cdots + a_np_n$ for some $a_i \in \mathfrak{a}$ and $p_i \in M$. Then we can compute

$$\varphi(y) - \varphi(x) \;=\; \varphi(p) \;=\; \sum_{i=1}^{n} a_i\varphi(p_i) \;\in\; \mathfrak{a}N$$

That is $\varphi(y) + \mathfrak{a}N = \varphi(x) + \mathfrak{a}N$, such that the map $\varphi/\mathfrak{a}$ truly is well-defined. The properties of being a homomorphism are straightforward: consider any $a \in R$ and any $x, y \in M$, then

$$\begin{aligned}
\varphi\left((a+\mathfrak{a})(x+\mathfrak{a}M)\right) &= \varphi(ax+\mathfrak{a}M) \;=\; \varphi(ax)+\mathfrak{a}N \\
&= a\varphi(x)+\mathfrak{a}N \;=\; (a+\mathfrak{a})\left(\varphi(x)+\mathfrak{a}N\right) \\
&= (a+\mathfrak{a})\varphi\left(x+\mathfrak{a}N\right) \\
\varphi\left((x+\mathfrak{a})+(y+\mathfrak{a}M)\right) &= \varphi\left((x+y)+\mathfrak{a}M\right) \;=\; \varphi(x+y)+\mathfrak{a}N \\
&= \varphi(x)+\varphi(y)+\mathfrak{a}N \\
&= \left(\varphi(x)+\mathfrak{a}N\right)+\left(\varphi(y)+\mathfrak{a}N\right)
\end{aligned}$$

(vii) If $\varphi : M \to N$ is surjective, then clearly $\varphi/\mathfrak{a} : M/\mathfrak{a}M \to N/\mathfrak{a}N$ is surjective as well: given any $y + \mathfrak{a}N \in N/\mathfrak{a}N$ we choose any $x \in M$ with $\varphi(x) = y$, then $(\varphi/\mathfrak{a})(x + \mathfrak{a}M) = \varphi(x) + \mathfrak{a}N = y + \mathfrak{a}N$.

If φ even is bijective, it remains to check the injectivity of $\varphi/\mathfrak{a}$. To do this we regard the following homomorphism of R-modules

$$\psi \;:\; M \to {}^{N}\Big/_{\mathfrak{a}N} \;:\; x \mapsto \varphi(x) + \mathfrak{a}N$$

That is $\psi = \pi\varphi$, where π denotes the canonical projection of N onto $N/\mathfrak{a}N$. Now by definition of ψ we see $\ker(\psi) = \{\, x \in M \mid \varphi(x) \in \mathfrak{a}N \,\}$ and therefore $\mathfrak{a}M \subseteq \ker(\psi)$. If conversely $\varphi(x) \in \mathfrak{a}N$, then $\varphi(x) = a_1y_1 + \cdots + a_ny_n$ for some $a_i \in \mathfrak{a}$ and $y_i \in N$. Yet as φ is bijective we may define $x_i := \varphi^{-1}(y_i)$, that is $y_i = \varphi(x_i)$ and hence

$$\varphi(x) \;=\; a_1\varphi(x_1) + \ldots a_n\varphi(x_n) \;=\; \varphi(a_1x_1 + \cdots + a_nx_n) \;\in\; \varphi(\mathfrak{a}M)$$

By the bijectivity of φ this means $x \in \mathfrak{a}M$ again, such that we have proved $\ker(\psi) = \mathfrak{a}M$. Now note that - by definiton of ψ - we have $(\varphi/\mathfrak{a})(x + \mathfrak{a}M) = \psi(x)$. Therefore

$$\ker\left(\varphi\Big/_{\mathfrak{a}}\right) \;=\; \ker(\psi)\Big/_{\mathfrak{a}M} \;=\; \mathfrak{a}M\Big/_{\mathfrak{a}M} \;=\; 0 \;\in\; M\Big/_{\mathfrak{a}M}$$

That is $\varphi/\mathfrak{a}$ has zero-kernel and hence is injective. As the surjectivity has already been proved we found the bijectivity of $\varphi/\mathfrak{a}$.

(viii) Consider any elements $z_1, \dots, z_n \in Z$, then by definition of the scalar multiplication on $M/\mathfrak{a}M$ we already see the identity

$$\sum_{i=1}^{n}(a_i + \mathfrak{a})z_i \quad \sum_{i=1}^{n} a_i z_i$$

And as in both cases the $a_i \in R$ can be chosen completely arbitrary this implies that the R-linear hull of Z equals the $(R/\mathfrak{a})$-linear hull.

(ix) Clearly Q is an R-sub-module of $M/\mathfrak{a}M$ if and only if Q equals its R-linear hull. Likewise Q is an $(R/\mathfrak{a})$-sub-module of $M/\mathfrak{a}M$ if and only if Q equals its $(R/\mathfrak{a})$-linear hull. But by (viii) these linear hulls are equal, and hence we get

$$\begin{aligned} Q \in \mathrm{Subm}_R\left(M \Big/ \mathfrak{a}M\right) &\iff \mathrm{Lh}_R(Q) = Q = \mathrm{Lh}_{R/\mathfrak{a}}(Q) \\ &\iff Q \in \mathrm{Subm}_{R/\mathfrak{a}}\left(M \Big/ \mathfrak{a}M\right) \end{aligned}$$

Now the explicit description of the $(R/\mathfrak{a})$-sub-modules of $M/\mathfrak{a}M$ is just an application of the correspondence theorem (3.16) of modules.

(x) Since $\mathfrak{a} \subseteq \mathfrak{b}$ it is clear from the definition that $\mathfrak{a}M \subseteq \mathfrak{b}M$. And as both $P := \mathfrak{a}M$ and $Q := \mathfrak{b}M$ are sub-modules of M the claim is nothing but the third isomorphism theorem of modules (3.78.(iv)) applied to this situation.

□

Proof of (3.46):

(i) We only need to show the well-definedness of the scalar multiplication: Hence let us consider any $x \in M_t$ and $a + tR = b + tR$. That is $b - a \in tR$, say $b - a = tu$ for some $u \in R$. Then $(b-a)x = tux = utx = u0 = 0$ and hence $bx = ax$. But this aleady is $(a + tR)x = (b + tR)x$.

(ii) Basically this is just an application of the first isomorphism theorem of modules (3.78.(ii)). Clearly both M_t and M_t are sub-modules, as they are defined as $M_t = \mathrm{kn}(\mu_t)$ and $tM = \mathrm{im}(\mu_t)$ respectively and the isomorphism claimed here is precisely the induced isomorphism in said theorem.

(iii) If $x \in M_t$ then $t\varphi(x) = \varphi(tx) = \varphi(0) = 0$ such that $\varphi(x) \in N_t$. This already is $\varphi(M_t) \subseteq N_t$. Let us now assume that φ is bijective, then we consider any $y \in N_t$, that is $ty = 0$. Now let $x := \varphi^{-1}(y) \in M$, then we have $\varphi(tx) = t\varphi(x) = ty = 0$ and thereby $tx = 0$, such that $x \in M_t$. That is we also have $y = \varphi(x) \in \varphi(M_t)$.

(iv) Consider any $x \in M_t \subseteq M$. By assumption x has a unique decomposition in terms of $x = \sum_i x_i$ where $x_i \in P_i$ for any $i \in I$. Then we have $0 = tx = t\sum_i x_i = \sum_i tx_i$ and as $tx_i \in P_i$ this is the unique decomposition of $0 \in M$ in terms of the P_i. Due to the uniqueness this is $tx_i = 0$ and hence $x_i \in (P_i)_t$. That is any $x \in M_t$ has a unique decomposition in terms of the $(P_i)_t$, which had to be shown.

(v) Let us first deal with the well-definedness of $t\varphi$. That is we consider any two $(r_i + a_iR) = (s_i + a_iR)$. That is we have $s_i - r_i \in a_iR$ for any $i \in I$ and multiplying this equation with t we get $ts_i - tr_i \in ta_iR = b_iR$. As this is true for any $i \in I$ we already have $(tr_i + b_iR) = (ts_i + b_iR)$ and thus $t\varphi$ is well-defined. Also the homomorphism properties of $t\varphi$ are plain to see.

So let us next assume, that φ is surjective, then we need to show that $t\varphi$ is surjective, as well. Given any $y \in tM$ we write $y = tx$ and choose $(r_i + b_iR)$ such that $\varphi(r_i + b_iR) = x$. Then we get

$$t\varphi\Big(r_i + a_iR\Big) \;=\; \varphi\Big(tr_i + b_iR\Big) \;=\; t\varphi\Big(r_i + b_iR\Big) \;=\; tx \;=\; y$$

Finally suppose that φ is injective and that $t \in \text{NZD}(R)$ is a non-zero-divisor, then we need to show that $t\varphi$ is injective, as well. So consider any $(r_i + a_iR)$ with $\varphi(tr_i + b_iR) = 0$. As φ is injective this leaves $(tr_i + b_iR) = 0$ which is $tr_i \in b_iR = ta_iR$ for any $i \in I$. But as $t \in \text{NZD}(R)$ this implies $r_i \in a_iR$ for any $i \in I$ and hence $(r_i + a_iR) = 0$.

(vi) In the first part we will check the well-definedness of the homomorphism $\varphi : a + sR \mapsto ra + tR$. Take a look at $a + sR = b + sR$, this means $b - a \in sR$ and thereby $rb - ra = r(b - a) \in rsR = tR$, such that $ra + tR = rb + tR$. Also we find that $s(ra + tR) = sra + tR = ta + tR = 0 + tR$ such that $ra + tR \in (R/tR)_s$ again. The R-linearity is clear, as well: $(a + sR) + (b + sR) = (a + b) + sR \mapsto r(a + b) + tR = (ra + tR) + (rb + tR)$ and $u(a + sR) = ua + sR \mapsto rua + tR = u(ra + tR)$.

Let us now assume that $t = rs \in \text{NZD}(R)$ is a non-zero-divisor of R. This implies that r and $s \in \text{NZD}(R)$ are non-zero-divisors, as well. And from this we can deduce the injectivity of φ: Suppose $0 + tR = \varphi(a + sR) = ra + tR$, this means $ra \in tR = rsR$ and as $r \in \text{NZD}(R)$ this again implies $a \in sR$ such that $a + sR = 0 + sR$. That is we have shown that $\varphi(a + sR) = 0 + tR$ implies $a + sR = 0 + sR$, which in turn implies the injectivity of φ.

For the surjectivity consider any $v + tR \in (R/tR)_s$ that is $s(v + tR) = 0 + tR$. In other words $sv \in tR = rsR = srR$ and as $s \in \text{NZD}(R)$, as well this again implies $v \in rR$. That is we have $v = ru$ for some $u \in R$. But then we find $\varphi(u + sR) = ru + tR = v + tR$, which already is the surjectivity.

(vii) For the implication " $\Longrightarrow$ " we have $1 + tR \in R/tR = (R/tR)_s$ and hence $0 + tR = s(1 + tR) = s + tR$ such that $s \in tR$. But this already is $t \mid s$. Conversely we start with $t \mid s$ and with the same reasoning arrive at $s + tR = 0 + tR$. Thus for any $a \in R$ we get $s(a + tR) = a(s + tR) = a(0 + tR) = 0 + tR$ such that $a + tR \in (R/tR)_s$. This is $R/tR \subseteq (R/tR)_s$ and the converse inclusion is trivial.

(viii) First of all $(R/tR)_p = 0$ is equivalent to saying $p(a + tR) = 0 + tR$ implies $a + tR = 0 + tR$ which again is equivalent to $a \in tR$. So let us start with $p \not\mid t$, then we are given some $a + tR$ with $p(a + tR) = 0 + tR$ and need to show $a \in tR$. By assumption we then have $pa \in tR$, that is $pa = tv$ for some $v \in R$. In particular $p \mid pa = tv$ which implies $p \mid t$ or $p \mid v$, since p is a prime element of R. But as also $p \not\mid t$ this only leaves $p \mid v$ and hence there is some $u \in R$ such that $pu = v$. Then we have $pa = tv = tpu$ and hence $a = tu$ since $p \in \text{NZD}(R)$. But this is $a \in tR$, which had to be shown.

Conversely if $p \mid t$, then by (iv) we have an isomorphism of the R-modules $R/pR \xrightarrow{\sim} (R/tR)_p$. As p is prime it is not a unit and hence $R/pR \neq 0$. Thus in turn we find $(R/tR)_p \neq 0$, as well.

□

Proof of (3.71):

(ii) If $x, y \in \ker(\varphi)$ then $\varphi(ax) = \alpha(a)\varphi(x) = \alpha(a)0 = 0$ and hence $ax \in \ker(\varphi)$ for any $a \in R$. Likewise $\varphi(x+y) = \varphi(x) + \varphi(y) = 0+0 = 0$, such that $x+y \in \ker(\varphi)$ as well. Hence $\ker(\varphi)$ is an R-sub-module of M. Now we have the assumption that α is surjective and consider any $u, v \in \operatorname{im}(\varphi)$, that is $u = \varphi(x)$ and $v = \varphi(y)$ for some $x, y \in M$. Then $u + v = \varphi(x) + \varphi(y) = \varphi(x+y) \in \operatorname{im}(\varphi)$. And if $b \in S$ then - due to the surjectivity of α - we may choose some $a \in R$ with $b = \alpha(a)$. Then $bu = \alpha(a)\varphi(x) = \varphi(ax) \in \operatorname{im}(\varphi)$ again, and hence $\operatorname{im}(\varphi)$ is an S-sub-module of N.

(iii) φ is surjective iff for any $y \in N$ there is some $x \in M$ such that $\varphi(x) = y$. In other words that is $N \subseteq \operatorname{im}(\varphi)$. But as $\operatorname{im}(\varphi) \subseteq N$ is true in any case, this is equivalent to $\operatorname{im}(\varphi) = N$.

Likewise φ is injective, iff for any $x, y \in M$ we get the implication $\varphi(x) = \varphi(y) \implies x = y$. But since φ is R-linear, this can also be put as $\varphi(y - x) = 0 \implies y - x = 0$. Let us now substitute $p = y - x$, then this is equivalent to: $\varphi(p) = 0 \implies p = 0$ for any $p \in M$. In other words that is $\ker(\varphi) \subseteq \{0\}$. But as as $\{0\} \subseteq \ker(\varphi)$ is true in any case, this is equivalent to $\ker(\varphi) = \{0\}$.

(iv) By definition $u, v \in \varphi^{-1}(Q)$ means $\varphi(u), \varphi(v) \in Q$. And as $0_N \in Q$ and $\varphi(0_M) = 0_N$ we find $0_M \in \varphi^{-1}(Q)$. If now $a \in R$, then $\varphi(au) = \alpha(a)\varphi(u) \in Q$, as Q is an S-sub-module of N. Therefore $au \in \varphi^{-1}(Q)$ again. Likewise $\varphi(u+v) = \varphi(u) + \varphi(v) \in Q$ such that $u + v \in \varphi^{-1}(Q)$, as well. Altogether $\varphi^{-1}(Q)$ is a sub-module of M.

By definition $x, y \in \varphi(P)$ means $x = \varphi(u)$ and $y = \varphi(v)$ for some $u, v \in P$. Again, as $0_M \in P$ and $\varphi(0_M) = 0_N$ we find $0_N \in \varphi(P)$. If $b \in S$, then (as α was assumed to be surjective) there is some $a \in R$ with $\alpha(a) = b$. But then we get $bx = \alpha(a)\varphi(u) = \varphi(au) \in \varphi(P)$, as $au \in P$, since P is a sub-module. Likewise $x + y = \varphi(u) + \varphi(v) = \varphi(u+v) \in \varphi(P)$, as $u + v \in P$, since P is a sub-module. Altogether $\varphi(P)$ is a sub-module of N.

(v) It suffices to check the general case, as the case of R-modules is included via $\alpha = \beta = \mathbb{1}$, that is by leaving out α and β. Consider any $x, y \in L$ and any $a \in R$, then it is easy to compute $\psi\varphi(ax+y) = \psi(\varphi(ax+y)) = \psi(\alpha(a)\varphi(x) + \varphi(y)) = \beta(\alpha(a))\psi(\varphi(x)) + \psi(\varphi(y)) = \beta\alpha(a)\psi\varphi(x) + \psi\varphi(x)$.

(vi) We have to prove that $\varphi + \psi$ and $a\varphi$ are homomorphisms of R-modules again. To do this consider any $x, y \in M$ and $b \in R$, then it is easy to compute $(\varphi+\psi)(bx+y) = \varphi(bx+y) + \psi(bx+y) = b\varphi(x) + \varphi(y) + b\psi(x) + \psi(y) = b(\varphi(x) + \psi(x)) + \varphi(y) + \psi(y) = b(\varphi+\psi)(x) + (\varphi+\psi)(y)$. And as R is commutative, we also get $(a\varphi)(bx+y) = a(b\varphi(x) + \varphi(y)) = ab\varphi(x) + a\varphi(y) = ba\varphi(x) + a\varphi(y) = b(a\varphi)(x) + (a\varphi)(y)$.

(vii) We have to prove that $\varphi + \psi$ and $a\varphi$ are α-module-homomorphisms again. To do this consider any $x, y \in M$, $a \in S$ and $b \in R$, then it is easy to compute $(\varphi+\psi)(bx+y) = \varphi(bx+y) + \psi(bx+y) = \alpha(b)\varphi(x) + \varphi(y) + \alpha(b)\psi(x) + \psi(y) = \alpha(b)(\varphi(x) + \psi(x)) + \varphi(y) + \psi(y) = \alpha(b)(\varphi+\psi)(x) + (\varphi+\psi)(y)$. And as S is commutative, we also get $(a\varphi)(bx+y) = a(\alpha(b)\varphi(x) + \varphi(y)) = a\alpha(b)\varphi(x) + a\varphi(y) = \alpha(b)a\varphi(x) + a\varphi(y) = \alpha(b)(a\varphi)(x) + (a\varphi)(y)$.

(viii) We already know by (v) that $\operatorname{end}(M)$ is an R-module under the point-wise addition and scalar multiplication. Also for any $\varphi, \psi \in \operatorname{end}(M)$ the composition $\varphi\psi$ is a homomorphism again, due to (iv), and hence $\varphi\psi \in \operatorname{end}(M)$ again. Trivially $\mathbb{1}_M$ satisfies the property of a unit element $\varphi\mathbb{1}_M = \varphi = \mathbb{1}_M\varphi$ for any $\varphi \in \operatorname{end}(M)$. It remains to check the distributivity: Consider any φ, ψ

and $\chi \in \mathrm{end}(M)$ and any $x \in M$, then [since the addition $+$ is point-wise] we find

$$\begin{aligned}
\varphi(\psi+\chi) \,:\, x &\mapsto \varphi\big(\psi(x)+\chi(x)\big) \\
&= \varphi(\psi(x)) + \varphi(\chi(x)) \\
&= (\varphi\psi + \varphi\chi)(x) \\
(\varphi+\psi)\chi \,:\, x &\mapsto \big(\varphi+\psi\big)\big(\chi(x)\big) \\
&= \varphi(\chi(x)) + \psi(\chi(x)) \\
&= (\varphi\chi + \psi\chi)(x)
\end{aligned}$$

(ix) First of all $Q := \Phi(P) \leq_{\mathsf{m}} M$ is a sub-module of M, according to (iv). And for any $x, y \in M$ we see that $x + P = y + P$ is equivalent to $y - x \in P$. But as Φ is injective, this is equivalent to $\Phi(y) - \Phi(x) = \Phi(y - x) \in \Phi(P) = Q$, which again is equivalent to $\Phi(x) + Q = \Phi(y) + Q$. That is we have proved the well-definedness and injectivity of $x + P \mapsto \Phi(x) + Q$ at the same time. But as Φ is surjective, so is $x + P \mapsto \Phi(x) + Q$, altogether this is an isomorphism of R-modules.

(x) The properties of an R-module-homomorphism are easy to see, if $a \in R$ and $(a_x), (b_x) \in R^{\oplus X}$ then $\varrho(a(b_x)) = \varrho(ab_x) = \sum_x (ab_x)x = a\sum_x b_x x = a\varrho(b_x)$, by construcion of $R^{\oplus X}$, refer to (3.60) for details. Likewise we compute $\varrho((a_x) + (b_x)) = \varrho(a_x + b_x) = \sum_x (a_x + b_x)x = \sum_x a_x x + \sum_x b_x x = \varrho(a_x) + \varrho(b_x)$. And $\mathrm{im}(\varrho) = \mathrm{Lh}_R(X)$ is clear from the definition of $\mathrm{Lh}_R(X)$ and the construction of ϱ. Now ϱ is surjective, iff $\mathrm{Lh}_R(X) = \mathrm{im}(\varrho) = N$ and in the light of (3.61.(ii)) this is precisely the definiton that X generates M. Also we have seen that ϱ is injective, iff $\mathrm{kn}(\varrho) = 0$ and by construction of ϱ this means $\sum_x a_x x = 0 \implies \forall\, x \in X : a_x = 0$. This again is the R-linear independence of X. If ϱ is bijective, then any $x \in M$ has a unique representation $(a_x) \in R^{\oplus X}$ with $x = \varrho(a_x) = \sum_x a_x x$. And by (3.61.(vi)) this is equivalent to X being an R-basis of M.

□

Proof of (3.72):
In (i) the one direction: $\varphi = \psi$ implies $\varphi(x) = \psi(x)$ for any $x \in X$ is trivial. Conversely consider any $y \in M$. As X generates M there are some $x_i \in X$ and $a_i \in R$ such that $y = a_1 x_1 + \cdots + a_n x_n$. Now by the R-linearity of φ and ψ we find

$$\begin{aligned}
\varphi(y) &= \varphi\left(\sum_{i=1}^{n} a_i x_i\right) = \sum_{i=1}^{n} a_i \varphi(x_i) \\
&= \sum_{i=1}^{n} a_i \psi(x_i) = \varphi\left(\sum_{i=1}^{n} a_i x_i\right) = \psi(y)
\end{aligned}$$

And as $y \in M$ has been chosen arbitarily we have in fact proved $\varphi = \psi$. So it remains to prove statement (ii). As B is a basis of M it is clear - due to(3.61.(vi)) - that the representation $y = \sum_x a_x x$ is unique and hence φ is a well-defined map. It also is easy to see that this φ is R-linear (see below). But from this we already get the uniqueness, due to (i). As to R-linearity: given $u \in R$ and $y = \sum_x a_x x$ and $z = \sum_x b_x x \in M$ we clearly see that

$$\varphi(uy) = \varphi\left(\sum_{x \in B} u a_x x\right)$$

$$
\begin{aligned}
&= \sum_{x\in B} u a_x n(x) \;=\; u \sum_{x\in B} a_x n(x) \;=\; u\varphi(y)\\
\varphi(y+z) &= \varphi\left(\sum_{x\in B}(a_x+b_x)x\right)\\
&= \sum_{x\in B} a_x n(x) + \sum_{x\in B} b_x n(x) \;=\; \varphi(y)+\varphi(z)
\end{aligned}
$$

□

Proof of (3.73):
We have to prove that the push-forward ψ_* and pull-back φ^* truly are homomorphisms again. As (i) is contained in (iii) and likewise (ii) is contained in (iv) (as $\alpha = \beta = \mathbb{1}$ we just have to omit α and β) we will prove the latter two claims only. For (iii) we pick up any $a \in S$ and φ, $\varphi' \in \mathrm{mhom}_\alpha(L,M)$. Then for any $x \in L$ we get $\psi_*(a\varphi+\varphi')(x) = \psi(a\varphi(x)+\varphi'(x)) = \beta(a)\psi\varphi(x)+\psi\varphi(x) = (\beta(a)\psi\varphi+\psi\varphi')(x)$. And as this is true for any $x \in L$ we got $\psi_*(a\varphi+\varphi') = \beta(a)\psi\varphi+\psi\varphi' = \beta(a)\psi_*(\varphi)+\psi_*(\varphi')$. For (iv) the reasoning is quite similar, pick up any $b \in T$ and ψ, $\psi' \in \mathrm{mhom}_\beta(L,N)$. Then for any $x \in L$ we get $\varphi^*(b\psi+\psi')(x) = (b\psi+\psi')(\varphi(x)) = b\psi\varphi(x)+\psi'\varphi(x) = (b\psi\varphi+\psi'\varphi)(x)$. And as this is true for any $x \in L$ we get $\varphi^*(b\psi+\psi') = b\psi\varphi+\psi'\varphi = b\varphi^*(\psi)+\varphi^*(\psi')$. □

Proof of (3.74):
In the first part we need to show the claim $\mathrm{im}(\pi) = \{\, x \in M \mid \pi(x) = x \,\}$. The inclusion " $\supseteq$ " is trivial, if $x \in M$ satisfies $x = \pi(x)$, then $x \in \mathrm{im}(\pi)$ already. Conversely, if $x \in \mathrm{im}(\pi)$ then there is some $u \in M$ such that $x = \pi(u)$. But by assumption this yields $\pi(x) = \pi^2(u) = \pi(u) = x$.
For the second part, we have to prove, that M is the inner direct product of $\mathrm{im}(\pi)$ and $\mathrm{kn}(\pi)$. But clearly for any $x \in M$ we have $x = \pi(x) + x - \pi(x)$. Thereby $x \in \mathrm{im}(\pi)$ is clear and since $\pi(x-\pi(x)) = \pi(x)-\pi^2(x) = \pi(x)-\pi(x) = 0$ we also have $x-\pi(x) \in \mathrm{kn}(\pi)$. Thus we have established $M = \mathrm{im}(\pi)+\mathrm{kn}(\pi)$. On the other hand if $u \in \mathrm{im}(\pi)\cap\mathrm{kn}(\pi)$, then these properties mean $u = \pi(x)$ for some $x \in M$ and $\pi(u) = 0$. Therefore $0 = \pi(u) = \pi^2(x) = \pi(x) = u$, such that $\mathrm{im}(\pi)\cap\mathrm{kn}(\pi) = 0$. Together this means $M = \mathrm{im}(\pi)\oplus\mathrm{kn}(\pi)$. □

Proof of (3.76):

(i) The linearity can be seen with a simple computation based on the compositions of R^2: consider a, b, x and $y \in R$ all elements of R, then $\alpha((a,b)+(x,y)) = \alpha(a+x,b+y) = (a+x)+(b+y) = (a+b)+(x+y) = \alpha(a,b)+\alpha(x,y)$. Likewise $\alpha(a(x,y)) = \alpha(ax,ay) = ax+ay = a(x+y) = a\alpha(x,y)$. However - for example in the case $R = \mathbb{Z}$ - we have $\alpha(2\cdot 1,1) = \alpha(2,1) = 2+1 = 3$, whereas $2\alpha(1,1) = 2(1+1) = 2\cdot 2 = 4$. That is in the case $R = \mathbb{Z}$ we see that α is definitely not multilinear.

(ii) In this case the multi-linearity follows from the definition of the compositions on R^2: $\mu(a+b,x) = (a+b)x = ax+bx = \mu(a,x)+\mu(b,x)$ and $\mu(ax,y) = (ax)y = a(xy) = a\mu(x,y)$. Likewise we see that $\mu(a,x+y) = \mu(a,x)+\mu(a,y)$ and $\mu(x,ay) = a\mu(x,y)$ due to the commutativity of R. Hence μ is R-multilinear but in the case $R = \mathbb{Z}$ again definitely not R-linear: $\mu(2\cdot(1,1)) = \mu(2,2) = 2\cdot 2 = 4$, whereas $2\mu(1,1) = 2(1\cdot 1) = 2\cdot 1 = 2$.

(iii) The R-linearity is well known and a direct consequence of the definition of the compositions on R^2: $\pi_2((a,b)+(x,y)) = \pi_2(a+x,b+y) = b+y = \pi_2(a,b)+\pi_2(x,y)$ and likewise $\pi_2(a(x,y)) =$

$\pi_2(ax, ay) = ay = a\pi_2(x, y)$. Hence π_2 is R-linear, but in the case $R = \mathbb{Z}$ again not R-linear, since: $\pi_2(3, 1) = 1 \neq 3 = 3\pi_2(1, 1)$.

(iv) is purely definitional.

(v) The additivity of $(A, B) \mapsto AB$ was proved in (4.8.(ii)). The first argument $A \mapsto AB$ thereby clearly is R-linear, since $aA \mapsto (aA)B = a(AB)$, for the second argument $B \mapsto AB$ we need that R is commutative, since $bB \mapsto A(bB) = (Ab)B = (bA)B = b(AB)$.

□

Proof of (3.77):
For the implication (a) $\Longrightarrow$ (b) it suffices to prove, that the inverse map $\Psi := \Phi^{-1} : N \to M$ is a homomorphism of R-modules again. Regard any $u, v \in M$ and let $x := \Phi(u)$ and $y := \Phi(v)$. Then we compute $\Phi^{-1}(x + y) = \Phi^{-1}(\Phi(u) + \Phi(v)) = \Phi^{-1}\Phi(u + v) = u + v = \Phi^{-1}(x) + \Phi^{-1}(y)$. Thus Φ^{-1} respects the addition. And for any $a \in R$ we also find that $\Phi^{-1}(ax) = \Phi^{-1}(a\,\Phi(u)) = \Phi^{-1}\Phi(au) = au = a\,\Phi^{-1}(x)$. Thus Φ^{-1} also respects the scalar multiplication and thereby is a homomorphism of R-modules. The converse implication (b) $\Longrightarrow$ (a) is clear, in particular Ψ is an inverse mapping of Φ. The implication (b) $\Longrightarrow$ (c) is trivial - just let $\alpha := \Psi$ and $\beta := \Psi$. And for the converse (c) $\Longrightarrow$ (a) we simply compute: $\alpha = \alpha\mathbb{1}_N = \alpha(\Phi\beta) = (\alpha\Phi)\beta = \mathbb{1}_M\beta = \beta$. Thus letting $\Psi := \alpha = \beta$ we have $\Psi = \Phi^{-1}$, such that Φ is bijective. □

Proof of (3.78):

(i) We will first prove the well-definedness of $\overline{\varphi}$: if $x + P = y + P$, then $y - x \in P \subseteq \varphi^{-1}(Q)$ and hence $\varphi(y) - \varphi(x) = \varphi(y - x) \in Q$. This again is $\varphi(y) + Q = \varphi(x) + Q$, which had to be shown. To prove that $\overline{\varphi}$ is an R-module-homomorphism can be done in a straightforward computation: let $a \in R$ and $x, y \in M$, then

$$\begin{aligned}
\overline{\varphi}\,(a(x + P) + (y + P)) &= \overline{\varphi}((ax + y) + P) = \varphi(ax + y) + Q \\
&= (a\varphi(x) + \varphi(y)) + Q \\
&= a\,(\varphi(x) + Q) + (\varphi(y) + Q) \\
&= a\overline{\varphi}(x + P) + \overline{\varphi}(y + P)
\end{aligned}$$

(ii) First of all, let us abbreviate $K := \mathrm{kn}(\varphi)$. Then $\overline{\varphi}$ is well-defined, since if $x + K = y + K$, then $k := y - x \in K$ and hence - as $\varphi(k) = 0$

$$\overline{\varphi}(y + K) = \varphi(y) = \varphi(x + k) = \varphi(x) + \varphi(k) = \varphi(x) = \overline{\varphi}(x + K)$$

That $\overline{\varphi}$ is an R-module homomorphism can be shown in complete analogy to the argument used in (i):

$$\begin{aligned}
\overline{\varphi}\,(a(x + K) + (y + K)) &= \overline{\varphi}((ax + y) + K) = \varphi(ax + y) \\
&= a\varphi(x) + \varphi(y) = a\overline{\varphi}(x + K) + \overline{\varphi}(y + K)
\end{aligned}$$

By construction we have $\mathrm{im}(\overline{\varphi}) = \mathrm{im}(\varphi)$, such that the surjectivity of $\overline{\varphi}$ is trivial. It suffices to check

the injectivity: so let us regard any $x, y \in M$ such that $\varphi(x) = \overline{\varphi}(x+K) = \overline{\varphi}(y+K) = \varphi(y)$. That is $\varphi(y-x) = \varphi(y) - \varphi(x) = 0$ and hence $y - x \in \mathsf{kn}(\varphi) = K$, such that $x + K = y + K$.

(iii) Consider the canonical projection $\pi : M \to M/P$ given by $\pi(x) = x + P$. Let us denote the restricion of π to Q by φ, that is $\varphi : Q \to M/P : x \mapsto x + P$. Then we get

$$\begin{array}{rcccl} \mathsf{kn}(\varphi) & = & \{\, x \in Q \mid x \in P \,\} & = & P \cap Q \\ \mathsf{im}(\varphi) & = & \{\, x + P \mid x \in Q \,\} & = & {}^{P+Q}\big/_{P} \end{array}$$

So by the 1st isomorphism theorem φ induces an isomorphism $\overline{\varphi} : Q/\mathsf{kn}(\varphi) \xrightarrow{\sim} \mathsf{im}(\varphi)$, given to be $\overline{\varphi}(x + \mathsf{kn}(\varphi)) = x + P$ and this is precisely the isomorphism given in the claim.

(iv) Consider the identity $\mathbb{1} : M \to M$ on M. As $P \subseteq Q = \mathbb{1}^{-1}(Q)$ the identity induces the map $\varphi : M/P \to M/Q : x + P \mapsto x + Q$, according to (i). For this homomorphism it is clear, that

$$\begin{array}{rcccl} \mathsf{kn}(\varphi) & = & \{\, x + P \in Q \mid x \in Q \,\} & = & {}^{Q}\big/_{P} \\ \mathsf{im}(\varphi) & = & \{\, x + Q \mid x \in M \,\} & = & {}^{M}\big/_{Q} \end{array}$$

So by the 1st isomorphism theorem φ induces an isomorphism $\overline{\varphi} : (M/P)/\mathsf{kn}(\varphi) \xrightarrow{\sim} \mathsf{im}(\varphi)$, given to be $\overline{\varphi}((x + P) + \mathsf{kn}(\varphi)) = x + Q$, and this is precisely the inverse of the isomorphism given in the claim.

□

Proof of (3.80):
We will prove the equivalences by going from bottom to top, in circles, starting with (c) $\implies$ (b): Let $Q := \mathsf{kn}(\pi)$, then due to the assumption $P = \mathsf{im}(\pi)$ we get $M = \mathsf{im}(\pi) \oplus \mathsf{kn}(\pi) = P \oplus Q$ according to (3.74).
(b) $\implies$ (a): By assumption $M = P + Q$ any $x \in M$ can be written in the form $x = p + q$ for some $p \in P$ and $q \in Q$. And this decomposition is unique since $P \cap Q = 0$. Thus we get a well-defined homomorphism of modules by letting

$$\Phi \;:\; M \to P \oplus {}^{M}\big/_{P} \;\; x \mapsto (p,\; x + P)$$

Clearly any $p \in P$ has the decomposition $p = p + 0 \in P + Q$ such that $\Phi(P) = P \times \{\, 0 + P \,\}$. But this homomorphism also is injective: Suppose $\Phi(x) = 0 = (0, 0 + P)$ where $x = p + q$. Then this would mean $p = 0$ and $x + P = 0 + P$. The latter equation means $x \in P$, but as also $x = 0 + q \in Q$ we have $x \in P \cap Q = 0$ such that $x = 0$ itself. It remains to prove, that Φ also is surjective: Consider any $(u, v + P)$ in $P \oplus M/P$, then we decompose $v = p + q \in P + Q$ and define $x := u + q$. Then we get $x + P = u + q + P = p + q + P = v + P$ since $p - u \in P$. But thereby $\Phi(x) = (u, x + P) = (u, v + P)$.
(a) $\implies$ (c): Let us denote the canonical projection onto the first component by $\alpha : P \oplus M/P \to P \oplus M/P : (p, q + P) \mapsto (p, 0 + P)$. Then clearly $\alpha^2 = \alpha$ and we may define $\pi := \Phi^{-1}\alpha\Phi : M \to M$. This π is a homomorphism, since it is a composition of such and we immediately find

$$\pi^2 \;=\; \Phi^{-1}\alpha\Phi\Phi^{-1}\alpha\Phi \;=\; \Phi^{-1}\alpha^2\Phi \;=\; \Phi^{-1}\alpha\Phi \;=\; \pi$$

Thus π is a projection, too and it only remains to prove $\mathrm{im}(\pi) = P$. To see this consider any $x \in M$ and let us denote $(p, q+P) := \Phi(x)$. Then $\pi(x) = \Phi^{-1}\alpha(p, q+P) = \Phi^{-1}(p, 0+P)$ such that $\Phi\pi(x) = (p, 0+P) \in P \times \{\, 0+P \,\} = \Phi(P)$. As Φ is injective this implies $\pi(x) \in P$ such that we have established $\mathrm{im}(\pi) \subseteq P$. Conversely consider any $p \in P$, then by assumption we have $\Phi(p) \in \Phi(P) = P \times \{\, 0+P \,\}$, that is there is some $u \in P$ such that $\Phi(p) = (u, 0+P)$. Now compute $\pi(p) = \Phi^{-1}\alpha\Phi(p) = \Phi^{-1}\alpha(u, 0+P) = \Phi^{-1}(u, 0+P) = p$. In particular $p = \pi(p) \in \mathrm{im}(\pi)$ such that $P \subseteq \mathrm{im}(\pi)$, as well. □

Proof of (3.165):

(i) We basically only have to check the well-definedness of the composition: Given two elements (x_i) and (y_i) of the inverse limit, we have to check, that $(x_i y_i)$ is an element of the inverse limit, again. But for any $i \leq j \in I$ we find $\gamma_j^i(x_j y_j) = \gamma_j^i(x_j)\gamma_j^i(y_j)$ as γ_j^i is a homomorphism of groups and $\gamma_j^i(x_j)\gamma_j^i(y_j) = x_i y_i$, by assumption on the (x_i), (y_i). All the properties associativity, commutativity, neutral and inverse elements, are inherited by the direct product of the G_i generally, for obvious reasons. Thus the inverse limit is a (commutative) group, again.

(ii) By (i) the inverse limit of the M_i is a commutative group under addition $+$ again. We have to check the well-definedness of the scalar multiplication. As before in (i), we get $\mu_j^i(a x_j) = a\mu_j^i(x_j) = a x_i$ for any $a \in R$ and (x_i) in the inverse limit. This time, as μ_j^i was also assumed to be R-linear. Thus $(a x_i)$ is another element of the inverse limit and hence this is an R-sub-module of the direct product of the M_i.

(iii) By (i) the inverse limit of the R_i is a commutative group under addition $+$ again. And (i) also shows, that the inverse limit is a monoid under multiplication $\cdot$. Thus the inverse limit is a sub-ring of the direct product of the R_i and thereby a (commutative) ring, in itself.

(iv) Is an immediate consequence of (ii) - which turns the inverse limit into an R-module - and (iii) - which turns the inverse limit into a (commutative) ring. Thus the inverse limit is an R-sub-algebra of the direct product of the A_i and thereby an R-algebra in itself.

(v) As before let X_∞ abbreviate the inverse limit of (X_i, f_j^i). In a first step we prove, that $\mathcal{W}$ is a base of some topology: As for any $i \in I$ we have $\pi_i^{-1}(X_i) = X_\infty$ already, $\mathcal{W}$ covers X_∞. Fix some point $x \in X_\infty$ and consider base sets such that $x \in \pi_i^{-1}(U_i) \cap \pi_j^{-1}(U_j)$. We have to find a base set $\pi_k^{-1}(V) \in \mathcal{W}$ in between $x \in \pi_k^{-1}(V) \subseteq \pi_i^{-1}(U_i) \cap \pi_j^{-1}(U_j)$. As I is a net, there is some $k \in I$ with $k \geq i$ and $k \geq j$. Now define

$$V \;:=\; (f_k^i)^{-1}(U_i) \cap (f_k^j)^{-1}(U_j) \;\subseteq\; X_k$$

As the f_j^i are continuous, V is an open subset of X_k. And as $f_k^i \pi_k = \pi_i$ and likewise $f_k^j \pi_k = \pi_j$ we can compute

$$\begin{aligned} \pi_k^{-1}(V) &= \pi_k^{-1}(f_k^i)^{-1}(U_i) \cap \pi_k^{-1}(f_k^j)^{-1}(U_j) \\ &= (f_k^i \pi_k)^{-1}(U_i) \cap (f_k^j \pi_k)^{-1}(U_j) \\ &= \pi_i^{-1}(U_i) \cap \pi_j^{-1}(U_j) \end{aligned}$$

In particular $\pi_k^{-1}(V) \subseteq \pi_i^{-1}(U_i) \cap \pi_j^{-1}(U_j)$ and $x \in \pi_k^{-1}(V)$, such that $\mathcal{W}$ is the base of some topology, according to (6.12.(iii)). Now a set $C \subseteq X_\infty$ is closed, iff $C = X_\infty \setminus U$ for some open subset $U \subseteq X_\infty$. And by construction U has to be the union of open base sets taken from $\mathcal{W}$. That is there has to be some index set Λ such that $U_\lambda \subseteq X_{i(\lambda)}$ are open subsets, such that U is the union of $\pi_{i(\lambda)}^{-1}(U_\lambda)$. Let $C_\lambda := X_{i(\lambda)} \setminus U_\lambda$, then we compute

$$\begin{aligned} C &= X_\infty \setminus U = X_\infty \setminus \bigcup_{\lambda\in\Lambda} \pi_{i(\lambda)}^{-1}(U_\lambda) \\ &= \bigcap_{\lambda\in\Lambda} \pi_{i(\lambda)}^{-1}(C_\lambda)) = \bigcap_{i\in I} \bigcap_{i(\lambda)=i} \pi_i^{-1}(C_\lambda) \\ &= \bigcap_{i\in I} \pi_i^{-1}\left(\bigcap_{i(\lambda)=i} C_\lambda \right) \end{aligned}$$

So if we let C_i be the intersection of all C_λ with $i(\lambda) = i$ (that is $C_i = X_i$ in case there is no $\lambda \in \Lambda$ with $i(\lambda) = i$), then C is precisely of the form given in the claim.

□

Proof of (3.167):
We need to verify, that $\sim$ is an equivalence relation on $\mathcal{M}$, that is reflexive, symmetric and transitive: For any $i \in I$ and any $x \in M_i$ we have $\varphi_i^i(x) = x = \varphi_i^i(x)$ and hence $(i,x) \sim (i,x)$, which is the reflexivity. And for any $i, j \in I$ and any $x \in M_i$ and $y \in M_j$ such that $(i,x) \sim (j,y)$ there is some $p \geq i, j$ such that $\varphi_i^p(x) = \varphi_j^p(y)$. But this is $\varphi_j^p(y) = \varphi_i^p(x)$, which is the symmetry $(j,y) \sim (i,x)$. And if $(j,y) \sim (k,z)$, as well, then again there is some $q \in I$ with $j, k \leq q$ and $\varphi_j^q(y) = \varphi_k^q(z)$. Now choose some $r \in I$ with $p, q \leq r$, then we get $(i,x) \sim (k,z)$ from

$$\varphi_i^r(x) = \varphi_p^r\varphi_i^p(x) = \varphi_p^r\varphi_j^p(y) = \varphi_j^r(y) = \varphi_q^r\varphi_j^q(y) = \varphi_q^r\varphi_k^q(z) = \varphi_k^r(z)$$

That is $\sim$ also is transitive, altogether an equivalence relation. Let us also prove the commutativity of the diagram $\varepsilon_j\varphi_i^j = \varepsilon_i$ for any $i \leq j$: Consider any $x \in M_i$ and let $k := j$ and $y := \varphi_i^j(x) \in M_j$. Then $\varphi_i^k(x) = y = \varepsilon_j^k(y)$ and hence $(i,x) \sim (j,y)$. That is $\varepsilon_i(x) = [i,x] = [j,y] = [j,\varphi_i^j(x)] = \varepsilon_j\varphi_i^j(x)$ and hence $\varepsilon_i = \varepsilon_j\varphi_i^j$, as this is true for any $x \in M_i$. □

Proof of (3.168):

(i) Let us abbreviate $G_\infty := \varinjlim (G_i, \gamma_i^j)$. First of all we have to verify, that the composition $[i,x][j,y] := [k, \gamma_i^k(x)\gamma_j^k(y)]$ for some $k \geq i, j$ is well-defined: Consider any $(i_1,x_1) \sim (i_2,x_2)$ and $(j_1,y_1) \sim (j_2,y_2)$, then we have to show that $[i_1,x_1] + [j_1,y_1] = [i_2,x_2] + [j_2,x_2]$. By assumption we have some $p \geq i_1, i_2$ such that $\gamma_{i_1}^p(x_1) = \gamma_{i_2}^p(x_2)$ and some $q \geq j_1, j_2$ such that $\gamma_{j_1}^q(y_1) = \gamma_{j_2}^q(y_2)$. By definition $[i_1,x_1] + [j_1,y_1]$ is $[r_1, \gamma_{i_1}^{r_1}(x_1) + \gamma_{j_1}^{r_1}(y_1)]$ for some $r_1 \geq i_1, j_1$. Likewise there had to be some $r_2 \geq i_2, j_2$ such that $[i_2,x_2] + [j_2,y_2]$ has been defined, as $[r_2, \gamma_{i_2}^{r_2}(x_2) + \gamma_{j_2}^{r_2}(y_2)]$. Pick up any $s \geq r_1, r_2$ and $s \geq p, q$ then we compute

$$\gamma_{i_1}^s(x_1) = \gamma_p^s\gamma_{i_1}^p(x_1) = \gamma_p^s\gamma_{i_2}^p(x_2) = \gamma_{i_2}^s(x_2)$$

$$\gamma_{j_1}^s(y_1) = \gamma_q^s\gamma_{j_1}^q(y_1) = \gamma_q^s\gamma_{j_2}^q(y_2) = \gamma_{j_2}^s(y_2)$$

And from this we get

$$\gamma^s_{r_1}\big(\gamma^{r_1}_{i_1}(x_1)+\gamma^{r_1}_{j_1}(y_1)\big)=\gamma^s_{i_1}(x_1)+\gamma^s_{j_1}(y_1)=\gamma^s_{i_2}(x_2)+\gamma^s_{j_2}(y_2)=\gamma^s_{r_2}\big(\gamma^{r_2}_{i_2}(x_2)+\gamma^{r_2}_{j_2}(y_2)\big)$$

But this is $(r_1,\gamma^{r_1}_{i_1}(x_1)+\gamma^{r_1}_{j_1}(y_1))\sim(r_2,\gamma^{r_2}_{i_2}(x_2)+\gamma^{r_2}_{j_2}(y_2))$ and hence the composition on G_∞ is well-defined. All the properties associativity, commutativity, neutral and inverse elements, are inherited by G_∞ for obvious reasons: We check the associativity first: Given $[i,x]$, $[j,y]$ and $[k,z]$ choose $r\geq i,\,j$ and $s\geq r,\,k$, then we compute

$$\begin{aligned}\Big([i,x][j,y]\Big)[k,z] &= [r,\gamma^r_i(x)\gamma^r_j(y)][k,z] = [s,\gamma^s_r(\gamma^r_i(x)\gamma^r_j(y))\gamma^s_k(z)]\\ &= [s,(\gamma^s_i(x)\gamma^s_j(y))\gamma^s_k(z)] = [s,\gamma^s_i(x)(\gamma^s_j(y)\gamma^s_k(z))]\\ &= [s,\gamma^s_i(x)][s,\gamma^s_j(y)\gamma^s_k(z)] = [i,x]\Big([j,y][k,z]\Big)\end{aligned}$$

The commutativity of G_∞ (supposed all the G_i are commutative) is clear. For any $i\in I$ we have $[i,e_i][j,y]=[k,\gamma^k_i(e_i)\gamma^k_j(y)]=[k,e_k\gamma^k_j(y)]=[k,\gamma^k_j(y)]=[j,y]$ and this means that $[i,e_i]$ is a neutral element of G_∞. And clearly $[i,x][i,x^{-1}]=[i,xx^{-1}]=[i,e_i]$ (likewise $[i,x^{-1}][i,x]=[i,e_i]$) such that $[i,x^{-1}]$ is the inverse element of $[i,x]$. Altogether G_∞ is a (commutative) group again.

(ii) By (i) we know, that this addition turns the direct limit M_∞ into a commutative group again. What we have to do is check the well-definedness of the scalar multiplication: Given $a\in R$ and any $(i,x)\sim(j,y)$ we have to verify $[i,ax]=[j,ay]$. But by assumption there is some $k\geq i,\,j$ such that $\mu^k_i(x)=\mu^k_j(y)$. Multiplying this equation with a and using the R-linearity of the transition maps we find that

$$\mu^k_i(ax) = a\mu^k_i(x) = a\mu^k_j(y) = \mu^k_j(ay)$$

from which we get $(i,ax)\sim(j,ay)$. Thus the scalar multiplication also is well-defined and it remains to check the compatibility conditions (M) of an R-module. But these proves recycle the same ideas: Given $a\in R$, $[i,x]$ and $[j,y]$ we find the distributivity of the scalar multiplication from

$$\begin{aligned}a\Big([i,x]+[j,y]\Big) &= a[k,\mu^k_i(x)+\mu^k_j(y)] = [k,a(\mu^k_i(x)+\mu^k_j(y))]\\ &= [k,\mu^k_i(ax)+\mu^k_j(ay)] = [i,ax]+[j,ay] = a[i,x]+a[j,y]\end{aligned}$$

where $k\in I$ with $k\geq i,\,j$, as usual. Also $1[i,x]=[i,1x]=[i,x]$ is immediate from the construction. Likewise the associativity $(ab)[i,x]=[i,(ab)x]=[i,a(bx)]=a[i,bx]=a(b[i,x])$ for $a,\,b\in R$. And the distributivity of two scalars is straightforward to verify, as well:

$$(a+b)[i,x] = [i,(a+b)x] = [i,ax+bx] = [i,ax]+[i,bx] = a[i,x]+b[i,x]$$

(iii) By (i) above both, the addition $+$ and multiplication $\cdot$, of the direct limit R_∞ are well defined and satisfy the properties of a commutative group, resp. of a (commutative) monoid. The distributivity law in R_∞ is verified in complete analogy to the associativity of G_∞ in (i).

(iv) By (iii) above the direct limit A_∞ is a (commutative) ring under the addition and multiplication. Also A_∞ is an R-module under the scalar multiplication $a[i,f]=[i,af]$. The compatibility condition of the algebra A_∞ is straightforward again: Given $a\in R$ and $[i,f]$, $[j,g]\in A_\infty$ choose some $k\in I$

with $k \geq i, j$ and compute

$$\begin{aligned}
\Big(a[i,f]\Big)[j,g] &= [i,af][j,g] = [k,\alpha_i^k(af)\alpha_j^k(g)] = [k,a\alpha_i^k(f)\alpha_j^k(g)] \\
&= a[k,\alpha_i^k(f)\alpha_j^k(g)] = a\Big([i,f][j,g]\Big) \\
\Big(a[i,f]\Big)[j,g] &= [k,a\alpha_i^k(f)\alpha_j^k(g)] = [k,\alpha_i^k(f)\alpha_j^k(ag)] = [i,f][j,ag] = [i,f]\Big(a[j,g]\Big)
\end{aligned}$$

(v) All we have to do is verify that this construction truly yields a topology on X_∞. But $\emptyset \subseteq X_\infty$ is open, as for any $i \in I$ we have $\varepsilon_i^{-1}(\emptyset) = \emptyset \subseteq X_i$ is open and the same is true for X_∞ itself. Also the preimage ε_i^{-1} commutes with intersections and unions of sets and hence finite intersections and arbitrary unions of open sets in X_∞ are pulled back to finite intersections and arbitrary unions of open sets in X_i. And as the X_i are topological spaces these intersections resp. unions are open sets in X_i again.

□

Proof of (3.169):
In the case of topological spaces, the topology on X_∞ has been defined in exactly that manner, as to ensure that the ε_i are continuous. In the other cases we have to check the homomorphism properties: Pick up any $i \in I$ and any $x, y \in M_i$ then we compute

$$\varepsilon_i(x \cdot y) = [i, x \cdot y] = [i, \mu_i^i(x) \cdot \mu_i^i(y)] = [i,x] \cdot [i,y] = \varepsilon_i(x) \cdot \varepsilon_i(y)$$

where $\cdot$ is just any composition, not necessarily commutative. In case of R-modules and R-algebras we also have to check the R-linearity. So pick up some $a \in R$, as well, then

$$\varepsilon_i(ax) = [i, ax] = a[i,x] = a\varepsilon_i(x)$$

is even easier. So it only remains to prove: If all the maps $\mu_i^j : M_i \to M_j$ are injective, then so are the $\varepsilon_i : M_i \to M_\infty$. This is straightforward, once more: Given $x, y \in M_i$ with $\varepsilon_i(x) = \varepsilon_i(y)$ we have $[i,x] = [i,b]$ which is $\mu_i^j(x) = \mu_i^j(y)$ for some $j \geq i$. But as μ_i^j is injective, we conclude $x = y$, which is the injectivity of ε_i.

Consider topological spaces again: Suppose all of the μ_i^j are open maps, then we prove, that the ε_j are open, too. To do this we fix any $j \in I$ and an open subset $U \subseteq M_j$. We want to prove that $\varepsilon_j(U)$ is open, by definition this is the case, iff for any $i \in I$, the following set is an open subset of M_i

$$\begin{aligned}
\varepsilon_i^{-1}\Big(\varepsilon_j(U)\Big) &= \{\, x \in M_i \mid [i,x] \in \varepsilon_j(U) \,\} \\
&= \{\, x \in M_i \mid \exists\, u \in U : [i,x] \in [j,u] \,\} \\
&= \Big\{\, x \in M_i \mid \exists\, k \geq i, k\, \exists\, u \in U : \mu_i^k(x) = \mu_j^k(u) \,\Big\} \\
&= \Big\{\, x \in M_i \mid \exists\, k \geq i, k : \mu_i^k(x) \in \mu_j^k(U) \,\Big\} \\
&= \bigcup_{k \geq i,j} \Big\{\, x \in M_i \mid \mu_i^k(x) \in \mu_j^k(U) \,\Big\} \\
&= \bigcup_{k \geq i,j} (\mu_i^k)^{-1}\Big(\mu_j^k(U)\Big)
\end{aligned}$$

As by assumption all the μ_j^k are open and $U \subseteq M_j$ is open, so is $\mu_j^k(U)$. And as the μ_i^k also are continuous, we find that their preimages are open in M_i. And as any union of open sets is open, we found that $\varepsilon_i^{-1}(\varepsilon_j(U))$ is open, as needed. □

Proof of (3.170):
As (i) is a special case of (ii) it suffices to prove the latter: We already know that ε_m is a $\star$-morphism, according to (3.169). Let us verify, that the inverse map $\pi_m : [i,x] \mapsto \mu_i^m(x)$ is well-defined: Consider any $[i,x] = [j,y]$, that is $\mu_i^k(x) = \mu_j^k(y)$ for some $k \geq i, j$. By assumption we also have $m \geq k$, therefore

$$\mu_i^m(x) \;=\; \mu_k^m \mu_i^k(x) \;=\; \mu_k^m \mu_j^k(y) \;=\; \mu_j^m(y)$$

which means $[i,x]$ and $[j,y]$ are mapped to the same element of M_m under π_m. It is straightforward to check, that π_m is the inverse of ε_m: If we start with any $x \in M_m$, then $x \mapsto [m,x] \mapsto \mu_m^m(x) = x$ and if we start with some $[i,x]$ in the direct limit, then $[i,x] \mapsto \mu_i^m(x) \mapsto [m, \mu_i^m(x)] = [i,x]$. In particular ε_m is a bijective $\star$-morphism. This proves, that ε_m is an isomorphism for all the algebraic categories. For topological spaces we still have to verify, that ε_m also is an open map. If we consider any open subset $U \subseteq M_m$, then for any $i \in I$ we get (as ε_m is bijective)

$$\varepsilon_i^{-1}(\varepsilon_m(U)) \;=\; (\varepsilon_m \mu_i^m)^{-1}(\varepsilon_m(U)) \;=\; (\mu_i^m)^{-1}\varepsilon_m^{-1}(\varepsilon_m(U)) \;=\; (\mu_i^m)^{-1}(U)$$

As μ_i^m is continuous, this is an open subset of M_i and as this is true for any $i \in I$ (by defintion of the topology on the direct limit), this makes $\varepsilon_m(U)$ an open subset. Thus ε_m is open, continuous and bijective, which is a homeomorphism - an isomorphism of $\star$-objects. □

Proof of (3.171):

- The property $\iota_l^n = \iota_m^n \iota_l^m$ for any $l \leq m \leq n$ has been shown in proposition (8.15.(ii)) and hence $(R[n], \iota_m^n)$ is a direct system of commutative rings. It remains to prove the isomorphy of the direct limit $L := \varinjlim (R[n], \iota_m^n)$ to $R[\infty]$. We start by proving, that $[k,a] \mapsto \iota_k^\infty(a)$ is well-defined: That is we regard any $[k,a] = [l,b]$, that is $\iota_k^n(a) = \iota_l^n(b)$ for some $n \geq k, l$. But from this we get

 $$\iota_k^\infty(a) \;=\; \iota_n^\infty \iota_k^n(a) \;=\; \iota_n^\infty \iota_l^n(b) \;=\; \iota_l^\infty(b)$$

 It is plain to see, that this becomes a homomorphism of rings from L to $R[\infty]$. For example let us check the additivity of this map

 $$[k,a] + [l,b] \;=\; [n, \iota_k^n(a) + \iota_l^n(b)] \;\mapsto\; \iota_n^\infty\big(\iota_k^n(a) + \iota_l^n(b)\big) \;=\; \iota_k^\infty(a) + \iota_l^\infty(b)$$

- Let us define another map from $R[\infty]$ to L: Given $f \in R[\infty]$ we may invoke (8.15.(i)) to find a finite set $\Omega \subseteq I_\infty$ such that $f = \iota_\Omega^\infty(a)$ for some $a \in R[\Omega]$. As $\Omega \subseteq I_\infty$ is finite there is some $n \in \mathbb{N}$ such that $\Omega \subseteq I_n$ and hence $f = \iota_n^\infty(\check{f})$ for $\check{f} := \iota_\Omega^n(a)$. Let us define the map

 $$R[\infty] \;\to\; L \;:\; f \;\mapsto\; [n, \check{f}]$$

 where $\check{f} \in R[n]$ with $f = \iota_n^\infty(\check{f})$. We need to prove, that this is well defined: That is we suppose

$f = \iota_k^\infty(a)$ and $f = \iota_l^\infty(b)$ for some $a \in R[k]$ and $b \in R[l]$ respectively. Choose some $n \geq k, l$, then

$$\iota_n^\infty\big(\iota_k^n(a)\big) \;=\; \iota_n^\infty(f) \;=\; \iota_n^\infty\big(\iota_l^n(b)\big)$$

As ι_n^∞ is injective, we conclude $\iota_k^n(a) = \iota_l^n(b)$ and hence $[k,a] = [l,b]$, such that $f \mapsto [n,\check{f}]$ is well-defined. Let us now prove, that this map is the inverse of $[k,a] \mapsto \iota_k^\infty(a)$. Let us start with $f \in R[\infty]$, then this is mapped to

$$f \;\mapsto\; [n,\check{f}] \;\mapsto\; \iota_n^\infty(\check{f})$$

Thereby $\check{f} \in R[n]$ is chosen in such a way, that $\iota_n^\infty(\check{f}) = f$ such that f is mapped to f. Conversely, if we start with $[k,a] \in L$ then this is turned into

$$[k,a] \;\mapsto\; f := \iota_k^\infty(a) \;\mapsto\; [n,\check{f}]$$

Thereby we can chose $n = k$ and $\check{f} = a$, as $f = \iota_k^\infty(a)$ by construction. Thus $[k,a]$ is mapped to $[k,a]$ again. Altogether these maps are mutually inverse.

- Let us summarize: $[k,a] \mapsto \iota_k^\infty(a)$ is a homomorphism of rings and $f \mapsto [n,\check{f}]$ is its inverse map. That is $[k,a] \mapsto \iota_k^\infty(a)$ is bijective and hence an isomorphism.

□

Proof of (3.172):

(i) Consider any $[i,x] \in M_\infty$, that is $i \in I$ and $x \in M_i$. Then by assumption X_i generates M_i and hence there are some $a_1,\ldots,a_n \in R$ and $x_1,\ldots,x_r \in X_i$ such that $x = a_1x_1 + \cdots + a_nx_n$. And from this we see, that we can generate $[i,x]$ as an R-linear combination over X_∞:

$$[i,x] \;=\; \left[i, \sum_{r=1}^n a_r x_r\right] \;=\; \sum_{r=1}^n a_r [i,x_r] \;=\; \sum_{r=1}^n a_r \varepsilon_i(x_i)$$

(ii) Consider finitely many scalars $a_r \in R$ and elements $x_r \in X_{i(r)}$ (where $r \in 1\ldots n$ and $i(r) \in I$) such that the $[i(r),x_r] \in X_\infty$ are pairwise distinct. We have to prove, that these elements are R-linearly independent, hence we consider a relation of the form

$$0 \;=\; \sum_{r=1}^n a_r\, \varepsilon_{i(r)}(x_i) \;=\; \sum_{r=1}^n a_r [i(r),x_r] \;=\; \left[k, \sum_{r=1}^n a_r\, \mu_{i(r)}^k(x_r)\right]$$

for some $k \in I$ with $k \geq i(1),\ldots,i(n)$. The zero-element of M_∞ is given to be $0 = [j,0]$ for any $j \in I$ and $0 \in M_j$. Then we have $[j,0] = [k,z]$ if any only if $0 = \mu_j^m(0) = \mu_k^m(z)$. That is the above equation turns into

$$0 \;=\; \mu_k^m\left(\sum_{r=1}^n a_r \mu_{i(r)}^k(x_r)\right) \;=\; \sum_{r=1}^n a_r \mu_k^m \mu_{i(r)}^k(x_r) \;=\; \sum_{r=1}^n a_r \mu_{i(r)}^m(x_r)$$

Suppose we had $\mu_{i(1)}^m(x_1) = \mu_{i(2)}^m(x_2)$, then we had $[i(1),x_1] = [i(2),x_2]$ in contradiction to the $[i(r),x_r]$ being pairwise distinct. Thus the $\mu_{i(r)}^m(x_r)$ are pairwise distinct. But also $\mu_{i(r)}^m(x_r) \in$

$\mu^m_{i(r)}(X_{i(r)} \subseteq X_m$ by assumption (2). And as X_m is R-linearly independent, by assumption (1), we conclude $a_r = 0$ for any $r \in 1 \dots n$. In the end this means that the $[i(r), x_r]$ and hence X_∞ are R-linearly independent

(iii) Any R-basis X_i is R-linearly independent and hence X_∞ is R-linearly independent, according to (ii). Also any R-basis X_i generated M_i as an R-module and hence X_∞ generates M_∞ as an R-module, according to (i). Together this means X_∞ is an R-basis of M_∞ again.

□

Proof of (3.173):

(i) *Uniqueness:* First note, that for any $x = (x_i)$ and $y = (y_i) \in \mathcal{M}_\infty$ we have $x = y$ if and only if $\pi_i(x) = x_i = y_i = \pi_i(y)$ for any $i \in I$. Now suppose λ and λ' were any two maps making the diagrams $\lambda_i = \pi_i\lambda$ and $\lambda_i = \pi_i\lambda'$ commute (for any $i \in I$). Then for any $\ell \in L$ we find $\pi_i(\lambda(\ell)) = \lambda_i(\ell) = \pi_i(\lambda'(\ell))$ by the commutativity of the diagrams. And as this is true for any $i \in I$ we conclude $\lambda(\ell) = \lambda'(\ell)$. And therefore $\lambda = \lambda'$, as $\ell \in L$ has been arbitrary, too.

Existence: We have to define $\lambda : L \to M_\infty$ by $\lambda(\ell) := (\lambda_i(\ell))$. This obviously makes the diagrams $\lambda_i = \pi_i\lambda$ commute. We only have to check, that this yields a $\star$-morphism. By assumption all the μ^k_i and μ_i are $\star$-morphisms. So if $\cdot$ is any composition on $\star$-objects, then for any $i, j \in I$ and any $\ell, m \in L$ we may compute

$$\lambda(\ell \cdot m) \;=\; \Big(\lambda_i(\ell \cdot m)\Big) \;=\; \Big(\lambda_i(\ell) \cdot \lambda_i(m)\Big) \;=\; \Big(\lambda_i(\ell)\Big) \cdot \Big(\lambda_i(m)\Big) \;=\; \lambda(\ell) \cdot \lambda(m)$$

And if the $\star$-objects have a scalar multiplication over a commutative ring $(R, +, \cdot)$, then the computation is even more easy: Also consider any $a \in R$, then we find

$$\lambda(a\ell) \;=\; \Big(\lambda_i(a\ell)\Big) \;=\; \Big(a\lambda_i(\ell)\Big) \;=\; a\Big(\lambda_i(\ell)\Big) \;=\; a\lambda(\ell)$$

It remains to check the case of topological spaces, that is we need to prove, that λ is continuous. As $\mathcal{W}$ is a basis of the limit topology, it suffices to check this for any $\pi_i^{-1}(U)$ for some open subset $U \subseteq M_i$. But as λ_i is assumed to be continuous we find that the pre-image of $\pi_i^{-1}(U)$ under λ is open, from the commutativity of the diagram $\lambda_i = \pi_i\lambda$, as

$$\lambda^{-1}\Big(\pi_i^{-1}(U)\Big) \;=\; (\pi_i\lambda)^{-1}(U) \;=\; \lambda_i^{-1}(U) \;\subseteq\; L \text{ open}$$

(ii) *Uniqueness:* Suppose λ and λ' were any two maps making the diagrams $\lambda_i = \lambda\varepsilon_i$ and $\lambda_i = \lambda'\varepsilon_i$ commute (for any $i \in I$). Consider any element of M_∞, these are of the form $[i, x]$ for some $i \in I$ and $x \in M_i$. Then we already see, that $\lambda = \lambda'$ have to be equal, from

$$\lambda([i, x]) \;=\; \lambda\varepsilon_i(x) \;=\; \lambda_i(x) \;=\; \lambda'\varepsilon_i(x) \;=\; \lambda'([i, x])$$

Existence: We have to define $\lambda : M_\infty \to L$ by $\lambda([i, x]) := \lambda_i(x)$. Of course we have to check the well-definedness: If $[i, x] = [j, y]$ then there is some $k \geq i, j$ such that $\mu^k_j(x) = \mu^k_j(y)$ and hence $\lambda_i(x) = \lambda_k\mu^k_i(x) = \lambda_k\mu^k_j(y) = \lambda_j(y)$. Thus λ is constant on the the equivalence classes and hence

well-defined. It remains to verify the properties of a $\star$-morphism: By assumption all the μ_i^k and λ_i are $\star$-morphisms. So if $\cdot$ is any composition on $\star$-objects, then for any $i, j \in I$ and any $x \in M_i$, $y \in M_j$ we may compute

$$\begin{aligned}\lambda([i,x]\cdot[j,y]) &= \lambda([k,\mu_i^k(x)\cdot\mu_j^k(y)]) \;=\; \lambda_k(\mu_i^k(x)\cdot\mu_j^k(y)) \\ &= \lambda_k\mu_i^k(x)\cdot\lambda_k\mu_j^k(y) \;=\; \lambda_i(x)\cdot\lambda_j(y) \\ &= \lambda([i,x])\cdot\lambda([j,y])\end{aligned}$$

And if the $\star$-objects have a scalar multiplication over a commutative ring $(R,+,\cdot)$, then the computation is even more easy: Also consider any $a \in R$, then we find

$$\lambda(a[i,x]) \;=\; \lambda([i,ax]) \;=\; \lambda_i(ax) \;=\; a\lambda_i(x) \;=\; a\lambda([i,x])$$

It remains to check the case of topological spaces: Consider any open subset $U \subseteq L$, as λ_i is assumed to be continuous (a $\star$-morphism) $\lambda_i^{-1}(U) \subseteq M_\infty$ is open, too. But by assumption all the μ_i^j are open, such that the structure morphisms ε_i are open as well, according to (3.169). And from this we find, that λ is continuous, as we get

$$\lambda^{-1}(U) \;=\; \{\,[i,x] \in M_\infty \mid \lambda_i(x) \in U\,\} \;=\; \Big\{\,[i,x] \in M_\infty \mid x \in \lambda_i^{-1}(U)\,\Big\} \;=\; \bigcup_{i\in I} \varepsilon_i\Big(\lambda_i^{-1}(U)\Big)$$

□

Proof of (3.175):

(i) The isomorphism from $\hom(L,M_\infty)$ to H_∞ will be gained by the universal property of the inverse limit. After that it only remains to check that this $\star$-morphism is bijective.

Let us start with pointing out, that $(H_i,(\mu_j^i)_*)$ truly is an inverse system of $\star$-objects. First of all any $H_i = \hom(L,M_i)$ is a $\star$-object again. Note that R is assumed to be commutative, then this has been shown for R-modules in (3.71.(vi)) and the same arguments apply to other $\star$-objects. Also the $(\mu_j^i)_*$ are $\star$-morphisms. This has been proved for R-modules again, in (3.73.(i)). As $\mu \mapsto \mu_*$ is order preserving, the inverse system is turned into an inverse system, again.

We will now prove, that $(\hom(L,M_\infty),(\pi_i)_*)$ is a target of the inverse limit H_∞, where the $\star$-morphisms $(\pi_i)_* : \hom(L,M_\infty) \to H_i$ are defined, by $(\pi_i)_*(\psi) := \pi_i\psi$. To do this, we have to show $(\pi_i)_* = (\mu_j^i)_*((\pi_j)_*)$ for any $i \le j \in I$. So consider any $\psi \in \hom(L,M_\infty)$ and compute

$$\big((\mu_j^i)_*((\pi_j)_*)\big)(\psi) \;=\; (\mu_j^i)_*\big((\pi_j)_*(\psi)\big) \;=\; (\mu_j^i)_*(\pi_j\psi) \;=\; \mu_j^i\pi_j\psi \;=\; \pi_i\psi \;=\; (\pi_i)_*(\psi)$$

That is the requirements of the universal property (3.173.(i)) are met and hence there is a (uniquely determined) $\star$-morphism λ from $\hom(L,M_\infty)$ to H_∞, given by

$$\lambda(\psi) \;=\; \big((\pi_i)_*(\psi)\big) \;=\; \big(\pi_i\psi\big)$$

Next we prove that this λ is bijective, hence a $\star$-isomorphism: For the injectivity we regard any two ψ, $\psi' \in \hom(L,M_\infty)$, such that $\lambda(\psi) = \lambda(\psi')$. By construction of λ this is $\pi_j\psi = \pi_j\psi'$ for

any $j \in I$. Given $u \in L$ let $(x_i) := \psi(u)$ and likewise $(x'_i) := \psi'(u) \in M_\infty$. In particular

$$x_j \;=\; \pi_j((x_i)) \;=\; \pi_j\psi(u) \;=\; \pi_j\psi'(u) \;=\; \pi_j((x'_i)) \;=\; x'_j$$

for any $j \in I$. This means $\psi(u) = (x_i) = (x'_i) = \psi'(u)$ and hence $\psi = \psi'$ as $u \in L$ has been arbitrary. It remains to verify the surjectivity of λ. Note that this also establishes the explicit description of the inverse map, as given in the claim. Pick up any $(\psi_i) \in H_\infty$, note that by definition of the inverse limit this means $\psi_i = (\mu^i_j)_*(\psi_j) = \mu^i_j\psi_j$ for any $i \leq j \in I$. We need some $\psi \in \hom(L, M_\infty)$ such that $\lambda(\psi) = (\psi_i)$. That is $\pi_i\psi = \psi_i$ for any $i \in I$, by construction of λ. The obvious way to achieve this, is by taking $\psi(u) := (\psi_i(u))$ for any $u \in L$. As the ψ_i are $\star$-morphisms and the operations on M_∞ are point-wise, ψ becomes a $\star$-morphism, too. It only remains to check, that $(x_i) := \psi(u) \in M_\infty$ again. But we get this, as well, as for any $i \leq j \in I$

$$x_i \;=\; \psi_i(u) \;=\; \mu^i_j\psi_j(u) \;=\; \mu^i_j(x_j)$$

(ii) The idea is to prove, that $\hom(M_\infty, N)$ also satisfies the universal property of the inverse limit H_∞. As an universal property determines an object up to isomorphy, they have to be isomorphic. The proof will be nothing but a streamlined version of this idea: We will prove, that $\hom(M_\infty, N)$ is a target of H_∞ and present an inverse to the ensuing map λ:

Let us start with pointing out, that $(H_i, (\mu^j_i)^*)$ truly is an inverse system of $\star$-objects. First of all any $H_i = \hom(M_i, N)$ is a $\star$-object again. Note that R is assumed to be commutative, then this has been shown for R-modules in (3.71.(vi)) and the same arguments apply to other $\star$-objects. Also the $(\mu^j_i)^*$ are $\star$-morphisms. This has been proved for R-modules again, in (3.73.(ii)). As $\mu \mapsto \mu^*$ is order reversing, the direct system is turned into an inverse system.

Let us turn $\hom(M_\infty, N)$ into a target of H_∞: With the direct limit M_∞ come the structure morphisms $\varepsilon_i : M_i \to M_\infty$. These give rise to $\varepsilon^*_i : \hom(M_\infty, N) \to H_i : \psi \mapsto \psi\varepsilon_i$. And as $\varepsilon_i = \varepsilon_j\mu^j_i$ we find that the ε^*_i also satisfy requirement (3) in the universal property of the indirect limit of $(H_i, (\mu^j_i)^*)$ as for any $\psi \in \hom(M_\infty, N)$ we can compute

$$\varepsilon^*_i(\psi) \;=\; \psi\varepsilon_i \;=\; \psi\varepsilon_j\mu^j_i \;=\; (\varepsilon_j\mu^j_i)^*(\psi) \;=\; \big((\mu^j_i)^*\varepsilon^*_j\big)(\psi)$$

Thus by (3.173.(i)) there is a (uniquely defined) $\star$-morphism $\lambda : \hom(M_\infty, N) \to H_\infty$ making the diagrams $\varepsilon^*_i = \pi_i\lambda$ commute, where $\pi_i : H_\infty \to H_i$ are the canonical projections. For some $\psi \in \hom(M_\infty, N)$ this λ is given to be

$$\lambda(\psi) \;\;=\;\; \big(\varepsilon^*_i(\psi)\big) \;\;=\;\; \big(\psi\varepsilon_i\big)$$

By this we have establishes the one side of the isomorphism, to be. Let us now define its inverse, to be - we call it μ. Given $\overline{\psi} := (\psi_i) \in H_\infty$ we define

$$\mu(\overline{\psi}) \;:=\; \Big([i,x] \mapsto \psi_i(x)\Big) \;\in\; \hom(M_\infty, N)$$

Of course we first have to check the well-definedness of this map: That is (1) $\psi_i(x)$ may not depend on the choice of $[i,x]$ and $[i,x] \mapsto \psi_i(x)$ has (2) to be a $\star$-homomophism. Note that this is precisely

the map λ occurring in (3.173.(ii)), so we only have to redo the arguments there: Let us address (1) first: Suppose $[i,x] = [j,y]$ for some $i, j \in I$ and $x \in M_i$, $y \in M_j$. That is there is some $k \geq i, j$ such that $\mu_i^k(x) = \mu_j^k(y)$. And as $(\psi_i) \in H_\infty$ this means, that for any $i \leq k$ we have $\psi_i = (\mu_i^k)^*(\psi_j) = \psi_j \mu_i^j$. In particular we can compute

$$\psi_i(x) \;=\; \psi_k \mu_i^k(x) \;=\; \psi_k \mu_j^k(y) \;=\; \psi_j(y)$$

And for the same reason we get the homomorphism property (2) of $\overline{\mu} := \mu(\overline{\psi})$. Let $+$ be any composition of the $\star$-objects, then $[i,x] + [j,y]$ has been defined to be $[k, \mu_i^k(x) + \mu_j^k(y)]$, for some $k \geq i, j$ again. Thus, as $\mu_k \in H_k$ is a $\star$-morphism, we find

$$\overline{\mu}\big([i,x] + [i,y]\big) \;=\; \psi_k\big(\mu_i^k(x) + \mu_j^k(y)\big) \;=\; \psi_k \mu_i^k(x) + \psi_k \mu_j^k(y) \;=\; \psi_i(x) + \psi_j(y)$$

which is $\overline{\mu}([i,x]) + \overline{\mu}([j,y])$ again. If needed, the R-linearity is even easier again: By scalar multiplication on M_∞ we simply have $\overline{\mu}(a[i,x]) = \overline{\mu}([i,ax]) = \psi_i(ax) = a\psi_i(x) = a\overline{\mu}([i,x])$.

It remains to prove, that these maps λ and μ are mutually inverse: Let us start with $\overline{\psi} = (\mu_i) \in H_\infty$, then we have to show $\lambda\mu(\overline{\psi}) = \overline{\psi}$. Let $\psi := \mu(\overline{\psi})$, then $\lambda\mu(\overline{\psi}) = \lambda(\psi) = (\psi\varepsilon_i)$. That is we have to show $\psi\varepsilon_i = \psi_i \in H_i$ for any $i \in I$. But this is clear, as for any $x \in M_i$ we have $\psi\varepsilon_i(x) = \psi([i,x]) = \mu(\overline{\psi})([i,x]) = \psi_i(x)$. And as this is true for any $x \in M_i$ we have $\psi\varepsilon_i = \psi_i$ and thereby $\lambda\mu$ is the identity on H_∞, as needed.

For the converse direction we start with some $\psi \in \hom(M_\infty, N)$ and have to prove $\mu\lambda(\psi) = \psi$. Let $\psi_i := \psi\varepsilon_i \in H_i$, that is $\overline{\psi} := \lambda(\psi) = (\psi_i)$. Now take a look at $\mu(\overline{\psi})$, by construction this maps $[i,x] \mapsto \psi_i(x) = \psi\varepsilon_i(x) = \psi([i,x])$. Thus $\mu(\overline{\psi})$ and ψ map any $[i,x]$ to the same element and hence are equal $\psi = \mu(\overline{\psi}) = \mu\lambda(\psi)$. That is $\mu\lambda$ also is the identity, as needed. In the end λ is a bijective $\star$-morphism with inverse map μ and thereby a $\star$-isomorphism.

□

Proof of (3.177):

(i) Let us first check the well-definedness of φ_∞: If we start with some $(x_i) \in M_\infty$ we have to check that $(y_i) := (\varphi_i(x_i)) \in N_\infty$ again. To do this regard any $i \leq j \in I$, then we have $\mu_j^i(x_j) = x_i$ and thereby can compute

$$\nu_j^i(y_j) \;=\; \nu_j^i \varphi_j(x_j) \;=\; \varphi_i \mu_j^i(x_j) \;=\; \varphi_i(x_i) \;=\; y_i$$

For inverse systems of algebraic $\star$-object, the compositions are point-wise. And as all the φ_i are $\star$-morphisms, φ_∞ respects these compositions. Thus for algebraic $\star$-objects, φ_∞ clearly is a $\star$-morphism, again. It remains to check the case of topological spaces: Hereby $(I, \leq)$ has to be a net. We have to verify, that φ_∞ is continuous, again. To do this, it suffices to regard open base sets of the topology, that is sets of the form $\pi_j^{-1}(V_j)$ for some open set $V_j \subseteq N_j$. But an easy computation shows, that the preimages of such sets, are open in M_∞ again

$$\varphi_\infty^{-1}\big(\pi_j^{-1}(V_j)\big) \;=\; \varphi_\infty^{-1}\Big(\big\{ (y_i) \in N_\infty \mid y_j \in V_j \big\} \Big)$$

$$
\begin{aligned}
&= \left\{ (x_i) \in M_\infty \mid \varphi_j(x_j) \in V_j \right\} \\
&= \left\{ (x_i) \in M_\infty \mid x_j \in \varphi_j^{-1}(V_j) \right\} \\
&= \pi_j^{-1}\big(\varphi_j^{-1}(V_j)\big)
\end{aligned}
$$

(ii) We first have to check the well-definedness of φ_∞ again: Consider any $[i,u]$, $[j,x] \in M_\infty$, then we have to verify $[i,\varphi_i(u)] = [j,\varphi_j(x)]$. By assumption there is some $k \geq i, j$ such that $\mu_i^k(u) = \mu_j^k(x)$. If we apply φ_k to this identity, we get $\nu_i^k\varphi_i(u) = \varphi_k\mu_i^k(u) = \varphi_k\mu_j^k(x) = \nu_j^k\varphi_j(x)$ which means $[i,\varphi_i(u)] = [j,\varphi_j(x)]$, as needed. For algebraic $\star$-objects the commutativity (2) of the diagrams also is the reason for the homomorphism property of φ_∞: Consider any two $[i,u]$ and $[j,x] \in M_\infty$ and let $\cdot$ be the composition of the $\star$-objects. If $k \geq i, j$, then we find

$$
\begin{aligned}
\varphi_\infty\big([i,u]\cdot[j,x]\big) &= \varphi_\infty\big([k,\mu_i^k(u)\cdot\mu_j^k(x)]\big) \\
&= [k,\varphi_k(\mu_i^k(u)\cdot\mu_j^k(x))] \\
&= [k,\varphi_k\mu_i^k(u)\cdot\varphi_k\mu_j^k(x)] \\
&= [k,\nu_i^k\varphi_i(u)\cdot\mu_j^k\varphi_j(x)] \\
&= [i,\varphi_i(u)]\cdot[j,\varphi_j(x)] \\
&= \varphi_\infty\big([i,u]\big)\cdot\varphi_\infty\big([j,x]\big)
\end{aligned}
$$

As always, if the $\star$-objects have a scalar multiplication, the linearity is even easier to see: $\varphi_\infty(a[i,u]) = \varphi_\infty([i,au]) = \varphi_i(au) = a\varphi_i(u) = a\varphi_\infty([i,u])$. It remains to treat topological spaces, where we assume the ν_i^j to be open, again. To prove, that φ_∞ is continuous we pick up an open subset $V \subseteq N_\infty$ and have to prove, that $\varphi_\infty^{-1}(V) \subseteq M_\infty$ is open again. That is we have to regard the pre-images $\varepsilon_i^{-1}(\varphi_\infty^{-1}(V))$. Choose any $i \in I$ and $x \in M_i$ then

$$
\begin{aligned}
x \in \varepsilon_i^{-1}(\varphi_\infty^{-1}(V)) &\iff [i,x] \in \varphi_\infty^{-1}(V) \\
&\iff [i,\varphi_i(x)] \in V \\
&\iff \exists\, [j,y] \in V \,:\, [i,\varphi_i(x)] = [j,y] \\
&\iff \exists\, [j,y] \in V\ \exists\, k \geq i,j \,:\, \nu_i^k\varphi_i(x) = \nu_j^k(y) \\
&\iff \exists\, [j,y] \in V\ \exists\, k \geq i,j \,:\, \varphi_k\mu_j^k(x) = \nu_j^k(y) \\
&\iff \exists\, \varepsilon_j(y) \in V\ \exists\, k \geq i,j \,:\, x \in (\mu_j^k)^{-1}\varphi_k^{-1}\nu_j^k(y) \\
&\iff \exists\, y \in \varepsilon_j^{-1}(V)\ \exists\, k \geq i,j \,:\, x \in (\mu_j^k)^{-1}\varphi_k^{-1}\nu_j^k(y) \\
&\iff \exists\, j \in I\ \exists\, k \geq i,j \,:\, x \in (\mu_j^k)^{-1}\varphi_k^{-1}\nu_j^k\varepsilon_j^{-1}(V)
\end{aligned}
$$

As $V \subseteq N_\infty$ is open, $\varepsilon_j^{-1}(V) \subseteq N_j$ is open by definition of the topology. As ν_j^k is open, φ_k and μ_j^k are continuous, this means, that $\varepsilon_i^{-1}(\varphi_\infty^{-1}(V))$ - and thereby $\varphi_\infty^{-1}(V)$ - is open, as we have seen

$$
\varepsilon_i^{-1}(\varphi_\infty^{-1}(V)) = \bigcup_{j\in I}\bigcup_{k\geq i,j} (\mu_j^k)^{-1}\varphi_k^{-1}\nu_j^k\varepsilon_j^{-1}(V)
$$

□

Proof of (3.178):

(i) It is quite easy to see, that φ_∞ is injective again: To say that $(x_i) \in \mathrm{kn}(\varphi_\infty)$ means $\varphi_i(x_i) = 0$ for any $i \in I$. But as all the φ_i are injective, we conclude $x_i = 0$ which is $(x_i) = 0$ and hence the injectivity of φ_∞. It only remains to verify $\mathrm{im}(\varphi_\infty) = \mathrm{kn}(\psi_\infty)$. By assumption all i-th chains are exact and hence $\mathrm{im}(\varphi_i) = \mathrm{kn}(\psi_i)$. Thus $\psi_i(y_i) = 0$ (for some $y_i \in M_i$) means there is some $x_i \in L_i$ such that $y_i = \varphi_i(x_i)$. Using this equivalence we find

$$\begin{aligned} \mathrm{im}(\varphi_\infty) &= \{\, (\varphi_i(x_i)) \in M_\infty \mid (x_i) \in L_\infty \,\} \\ \mathrm{kn}(\psi_\infty) &= \{\, (y_i) \in M_\infty \mid \forall\, i \in I\ \exists\, x_i \in L_i \,:\, y_i = \varphi_i(x_i) \,\} \end{aligned}$$

The inclusion $\mathrm{im}(\varphi_\infty) \subseteq \mathrm{kn}(\psi_\infty)$ is obvious: Given $(y_i) := (\varphi_i(x_i))$ for any $i \in I$ there is some $x_i \in L_i$ such that $y_i = \varphi_i(x_i)$. Conversely for $\mathrm{im}(\varphi_\infty) \supseteq \mathrm{kn}(\psi_\infty)$ consider any $i \leq j \in I$. As $(y_i) \in M_\infty$ we have $\mu_j^i(y_j) = y_i$. Pick up any $x_i \in L_i$ such that $y_i = \varphi_i(x_i)$, then this turns into $\mu_j^i \varphi_j(x_j) = \varphi_i(x_i)$. But as (φ_i) is a homomorphism of R-module-systems this is $\varphi_i \lambda_j^i(x_j) = \varphi_i(x_i)$. Recall that φ_i is injective, by this we conclude $\lambda_j^i(x_j) = x_i$. And as this is true for all $i \leq j$ we find $(x_i) \in L_\infty$ and hence $(y_i) \in \mathrm{im}(\varphi_\infty)$.

(ii) Let us start with the injectivity of φ_∞: Consider any $[i,x] \in L_\infty$ such that $0 = \varphi_\infty([i,x]) = [i, \varphi_i(x)]$. Choose any $j \in I$, then $[j,0] = 0$ such that we have $[i,\varphi_i(x)] = [j,0]$ which means $\mu_i^k \varphi_i(x) = \mu_j^k(0) = 0$ for some $k \geq i, j$. As (φ_i) is a homomorphism of the direct systems, we get $\varphi_k \lambda_i^k(x) = 0$. But by assumption φ_k is injective and thereby $\lambda_i^k(x) = 0 = \lambda_j^k(0)$. From this we get $[i,x] = [j,0] = 0$ which is the injectivity of φ_∞.

The surjectivity of ψ_∞ is really easy: Pick up any $[i,z] \in N_\infty$ that is $i \in I$ and $z \in N_i$. As ψ_i is surjective, there is some $y \in M_i$ such that $\psi_i(y) = z$. From this we get $[i,z] = [i,\psi_i(y)]$ and this is $[i,z] = \psi_\infty([i,y])$. In particular ψ_∞ is surjective.

It only remains to prove $\mathrm{im}(\varphi_\infty) = \mathrm{kn}(\psi_\infty)$. So let us decode the content, of these sets. By construction, we have

$$\begin{aligned} \mathrm{im}(\varphi_\infty) &= \{\, [i,\varphi_i(x)] \in M_\infty \mid i \in I,\, x \in L_i \,\} \\ \mathrm{kn}(\psi_\infty) &= \{\, [i,y] \in M_\infty \mid [i,\psi_i(y)] = 0 \,\} \end{aligned}$$

Hence the inclusion $\mathrm{im}(\varphi_\infty) \subseteq \mathrm{kn}(\psi_\infty)$ is easy to see: As $\psi_i \varphi_i(x) = 0$ for any $i \in I$ and any $x \in L_i$ we find that $[i,y] = [i,\varphi_i(x)]$ satisfies $[i,\psi_i(y)] = [i,\psi_i\varphi_i(x)] = [i,0] = 0$. For the converse inclusion, we start with some $[i,y]$ such that $[i,\psi_i(y)] = 0$. Again $0 = [j,0]$ for an arbitrary $j \in I$. From $[i,\psi_i(y)] = [j,0]$ we find some $k \geq i, j$ such that $\nu_i^k \psi_i(y) = \nu_j^k(0) = 0$. As (ψ_i) is a homomorphism of R-module-systems, this can be turned into $\psi_k \mu_i^k(y) = 0$, which is $\mu_i^k(y) \in \mathrm{kn}(\psi_k) = \mathrm{im}(\varphi_k)$. That is there is some $x_k \in L_k$ such that $\mu_i^k(y) = \varphi_k(x) = \mu_k^k \varphi_k(x)$. So we see $[i,y] = [k,\varphi_k(x)] \in \mathrm{im}(\varphi_\infty)$, the converse inclusiom.

□

Proof of (7.46):

- (a) $\Longrightarrow$ (b): consider any element $f \in \mathfrak{h}$ and pick up the homogeneous decomposition $f = \sum_d f_d$. By assumption (a) and as $f \in \mathfrak{h}$ we also find $h_d \in \mathfrak{h} \cap A_d$ such that f can be decomposed into $f = \sum_d h_d$. As f_d and $h_d \in A_d$ property (3) of graded algebras implies $f_d = h_d \in \mathfrak{h}$.

- (b) $\implies$ (c): For any $h \in \mathfrak{h}$ let us consider the homogeneous decomposition $h = \sum_d h_d$ and denote the set $H := \{\, h_d \mid h \in \mathfrak{h},\ h_d \neq 0 \,\}$. Then it is clear that $H \subseteq A_{\text{hom}}$, by definition of H. And by assumption (b) we have $H \subseteq \mathfrak{h}$. On the other hand any $h \in \mathfrak{h}$ has been decomposed as $h = \sum_d h_d \in \langle H \rangle_{\mathfrak{i}}$. And hence $\mathfrak{h} \subseteq \langle H \rangle_{\mathfrak{i}} \subseteq \mathfrak{h}$.

- (c) $\implies$ (a): Consider any $f \in \mathfrak{h} = \langle H \rangle_{\mathfrak{i}}$, that is there is a finite subset $\Omega \subseteq H$ and elements $g_h \in A$ (where $h \in \Omega$) such that $f = \sum_h g_h h$. For any $h \in \Omega$ let us abbreviate $d(h) := \deg(h)$ and pick up homogeneous decompositions $f = \sum_d f_d$ and $g_h = \sum_d g_{h,d}$. Then we compute

$$\sum_{d \in D} f_d \;=\; f \;=\; \sum_{h \in \Omega} \left(\sum_{d \in D} g_{h,d} \right) h \;=\; \sum_{d \in D} \sum_{h \in \Omega} g_{h,d} h$$

 As $g_{h,d}$ and h are homogeneous elements $g_{h,d}h$ is (either 0 or) a homogeneous element of degree $\deg(g_{h,d}h) = \deg(g_{h,d}) + \deg(h) = d + d(h)$. Thus we can split the sum over $(d,h) \in D \times \Omega$ into fibers (c,h) such that $c + d(h) = d$. Thereby we find

$$\sum_{d \in D} f_d \;=\; \sum_{d \in D} \sum_{c + d(h) = d} g_{h,c} h$$

 So on both sides of this equation we have homogeneous decompositions of f. Now by property (3) of graded algebrad this means that (for any $d \in D$) the homogeneous components have to coincide, too. That is

$$f_d \;=\; \sum_{c + d(h) = d} g_{h,c} h \;\in\; \mathfrak{h} \cap A_d$$

 Hence we have obtained that f can be decomposed as a sum of elements f_d contained in $\mathfrak{h} \cap A_d$. As f has been arbitrary that is $\mathfrak{h} = \sum_d \mathfrak{h} \cap A_d$. And as $\mathfrak{h} \cap A_d \subseteq A_d$ it is also clear that $(\mathfrak{h} \cap A_d) \cap (\sum_{c \neq d} \mathfrak{h} \cap A_c) \subseteq A_d \cap (\sum_{c \neq d} A_c) = 0$. Altogether we have obtained claim (a).

□

Proof of (7.40):
If f_k is homogeneous of degree $m - k$ then $f_k t_n^k$ is homogeneous of degree $(m-k)+k = m$. And as all these polynomials have the same degree m, the sum is homogeneous again. As $d = \deg_n(f)$ we have $f_d \neq 0$, Such that we have already established (b) $\implies$ (a). Conversely, as f is of degree $m = \deg(f)$, then the only multi-indices $\beta \in \mathbb{N}^n$ with $f[\beta] \neq 0$ satisfy $|\beta| \leq m$. If f also is homogeneous, then they even satisfy $|\beta| = m$. Therefore f is of the form

$$f \;=\; \sum_{|\beta| = m} f[\beta]\, t^\beta$$

Let us split $\beta \in \mathbb{N}^n$ up into $\beta = (\alpha, k)$, that is $k := \beta_n$ and $\alpha := (\alpha_1, \ldots, \alpha_{n-1})$. Then $|\alpha| = |\beta| - k = m - k$ such that we are able to rewrite f as

$$f \;=\; \sum_{k=0}^{d} \left(\sum_{|\alpha| = r-k} f[\alpha, k]\, t^\alpha \right) t^k$$

Here the polynomials in brackets are $f_k \in R[t_1, \ldots, t_{n-1}]$. As f was homogeneous we had $|\beta| = m$ which led to $|\alpha| = m - k$. Thus $f_k = 0$ or homogeneous of degree $m - k$. Note that $f_d \neq 0$, as f had a

coefficient $f[\beta] \neq 0$ for some $\beta = (\alpha, d)$. For a general polynomial we had $|\beta| \leq m$ instead and hence only $|\alpha| \leq m - k$ which yields $\deg(f_k) \leq m - k$ instead. □

Proof of (7.48):

(i) Let us write out the homogeneous decomposition $1 = \sum_d 1_d$. Then for any homogeneous element $h \in H$ - say $c := \deg(h)$ - we get

$$h \;=\; h \cdot 1 \;=\; \sum_{d \in D} h \cdot 1_d$$

Thereby $h \cdot 1_d \in A_{c+d}$ according to property (4). But as $h \in H$ is homogeneous we may compare coefficients (this is property (3)) to find $h = \sum_{c+d=c} h \cdot 1_d$. Yet D has been assumed to be integral, hence $c + d = c = c + 0$ implies $d = 0$. Thus for any $h \in H$ we have found $h = h \cdot 1_0$. Thus consider any $f \in A$ and decompose $f = \sum_d f_d$ into homogeneous elements. Then we compute

$$f \cdot 1_0 \;=\; \sum_{d \in D} f_d \cdot 1_0 \;=\; \sum_{d \in D} f_d \;=\; 0$$

as the $f_d \in H \cup \{0\}$ are homogeneous. Thus we have proved $f = f \cdot 1_0$ for *any* element $f \in A$. In particular $1 = 1 \cdot 1_0 = 1_0 \in A_0$.

(ii) Clearly the kernel is an ideal $\mathfrak{a} := \ker(\varphi) \trianglelefteq_{\mathrm{i}} A$ of A, so we only have to prove the graded property. First of all, it is clear that the sub-modules $\mathfrak{a} \cap A_d$ intersect trivially

$$(\mathfrak{a} \cap A_c) \cap \left(\sum_{d \neq c} \mathfrak{a} \cap A_d \right) \quad \subseteq \quad A_c \cap \left(\sum_{d \neq c} A_d \right) \quad = \quad \{0\}$$

Thus it remains to show that $\mathfrak{a}$ truly is the sum of the $\mathfrak{a} \cap A_d$. Consider any $f \in \mathfrak{a}$ and decompose f into homogeneous components $f = \sum_d f_d$ where $f_d \in A_d$. Then we get

$$0 \quad = \quad \varphi(f) \quad = \quad \sum_{d \in D} \varphi(f_d)$$

As φ was assumed to be graded, we have $\varphi(f_d) \in B_d$ again. Thus comparing homogeneous coefficients in B we find $\varphi(f_d) = 0$ for any $d \in D$. And this again translated into $f_d \in \mathfrak{a}$ such that $f_d \in \mathfrak{a} \cap A_d$. As f has been arbitrary this also shows

$$\mathfrak{a} \;=\; \sum_{d \in D} \mathfrak{a} \cap A_d$$

(iii) As $\mathfrak{a} \trianglelefteq_{\mathrm{i}} A$ is an ideal and A is an R-algebra, $\mathfrak{a} \trianglelefteq_{\mathrm{a}} A$ even is an R-algebra-ideal. And hence the quotient $A/\mathfrak{a}$ is an R-algebra again. And by construction we have $0 + \mathfrak{a} \notin (A/\mathfrak{a})_{\mathsf{hom}}$. Let us now prove the well-definedness of $\deg : (A/\mathfrak{a})_{\mathsf{hom}} \to D$: suppose we are given g and $h \in A$ such that $g + \mathfrak{a} = h + \mathfrak{a} \in (A/\mathfrak{a})_{\mathsf{hom}}$. That is $f := g - h \in \mathfrak{a}$. Let us now denote $b := \deg(g)$ and $c := \deg(h)$ and decompose $f = \sum_d f_d$ (where $f_d \in \mathfrak{a} \cap A_d$ by assumption). Then we find

$$\sum_{d \in D} \begin{cases} g \text{ if } d = b \\ 0 \text{ if } d \neq b \end{cases} \;=\; g \;\; f + h \;\; = \;\; \sum_{d \in D} \begin{cases} f_c + h \text{ if } d = c \\ f_d \text{ if } d \neq c \end{cases}$$

Now suppose we had $b \neq c$ then comparing coefficients we would find $g = f_b \in \mathfrak{a}$ in contradiction to $g + \mathfrak{a} \in (A/\mathfrak{a})_{\text{hom}}$. Thus we have $\deg(g) = b = c = \deg(h)$ and hence $\deg : (A/\mathfrak{a})_{\text{hom}} \to D$ is well-defined. We will now prove the identity

$$\left(A \Big/ \mathfrak{a}\right)_d \;=\; A_d + \mathfrak{a} \Big/ \mathfrak{a}$$

For the inclusion "$\subseteq$" we are given some $h + \mathfrak{a} \in (A/\mathfrak{a})_d$. If thereby $h + \mathfrak{a} = 0 + \mathfrak{a}$ then $h \in \mathfrak{a}$ and hence $h + \mathfrak{a} \in (A_d + \mathfrak{a})/\mathfrak{a}$. If on the other hand $h + \mathfrak{a} \neq 0 + \mathfrak{a}$ then we have $\deg(h) = d$ by assumption and hence $h \in A_d$. Altogether $h + \mathfrak{a} \in (A_d + \mathfrak{a})/\mathfrak{a}$ again. Conversely "$\supseteq$" consider any $h \in A_d$ and any $f \in \mathfrak{a}$. Then we have to show $(h + f) + \mathfrak{a} \in (A/\mathfrak{a})_d$. If $h = 0$ then $(h + f) + \mathfrak{a} = 0 + \mathfrak{a} \in (A/\mathfrak{a})_d$ is clear. And if $h \neq 0$ then $\deg(h) = d$ by assumption such that $(h + f) + \mathfrak{a} = h + \mathfrak{a}$ is of degree d, as well. Thus we have established the equality and in particular $(A/\mathfrak{a})_d$ is an R-sub-module of $A/\mathfrak{a}$. Now consider $g \in A_c$, $h \in A_d$ and a, $b \in \mathfrak{a}$. Then $(g + a)(h + b) = gh + (ah + gb + ab) \in A_{c+d} + \mathfrak{a}$. And as all these elements have been arbitrary this also proves property (4) of graded algebras, that is $(A/\mathfrak{a})_c (A/\mathfrak{a})_d \subseteq (A/\mathfrak{a})_{c+d}$. Now

$$A \Big/ \mathfrak{a} \;=\; \sum_{d \in D} A_d + \mathfrak{a} \Big/ \mathfrak{a}$$

is easy to see: if we are given any $f + \mathfrak{a} \in A/\mathfrak{a}$ then we may decompose $f = \sum_d f_d$ into homogeneous components. Thereby $f + \mathfrak{a} = \sum_d (f_d + \mathfrak{a})$. This already yields "$\subseteq$" and the converse inclusion is clear. Now fix any $c \in D$ then it remains to prove

$$\left(A_c + \mathfrak{a} \Big/ \mathfrak{a}\right) \cap \left(\sum_{d \neq c} A_d + \mathfrak{a} \Big/ \mathfrak{a}\right) \;=\; \{\, 0 + \mathfrak{a} \,\}$$

Thus consider any $f + \mathfrak{a}$ contained in the intersection. In particular that is $f + \mathfrak{a} \in (A_c + \mathfrak{a})/\mathfrak{a}$ and hence there is some $f_c \in A_c$ such that $f + \mathfrak{a} = f_c + \mathfrak{a}$. And likewise there are $f_d \in A_d$ (where $d \neq c$) such that $f + \mathfrak{a} = \sum_{d \neq c} f_d + \mathfrak{a}$. Thus we find

$$a \;:=\; f_c - \sum_{d \neq c} f_d \;\in\; \mathfrak{a} \;=\; \bigoplus_{d \in D} \mathfrak{a} \cap A_d$$

as $\mathfrak{a}$ has been assumed to be a graded ideal we can decompose a into $a = \sum_d a_d$ where $a_d \in \mathfrak{a} \cap A_d$. Comparing the homogeneous coefficients of a in A we find $f_c = a_c \in \mathfrak{a} \cap A_c$. In particular $f + \mathfrak{a} = f_c + \mathfrak{a} = 0 + \mathfrak{a}$, which had to be shown.

(iv) As U is multiplicatively closed $U^{-1}A$ is a commutative R-algebra under $a(f/u) = (af/u)$. And from the construction of $(U^{-1}A)_{\text{hom}}$ we also have $0 = 0/1 \notin (U^{-1}A)_{\text{hom}}$. As D was assumed to be a group $\deg : (U^{-1}A)_{\text{hom}} \to D$ is a well-defined map. (If D only was a monoid we would have to regard $\deg : (U^{-1}A)_{\text{hom}} \to \text{gr}D$ given by $\deg(h/u) := (\deg(h), \deg(u))$ instead). Next we prove

$$\left(U^{-1}A\right)_d \;=\; \left\{ \frac{h}{u} \;\middle|\; u \in U,\, h \in A_{d + \deg(u)} \right\}$$

The inclusion "$\supseteq$" is easy: the case $h/u = 0/1$ is clear and if $h/u \neq 0/1$ we particularly have $h \neq 0$. Hence $\deg(h) = \deg(u) + d$ by assumption on h and hence $\deg(h/u) = \deg(h) - \deg(u) = d$.

The converse "$\subseteq$" is analogous: the case $h/u = 0/1$ is clear again, as $0 \in A_{d+\deg(u)}$. And if $h/u \neq 0/1$ then $d = \deg(h/u) = \deg(h) - \deg(u)$ and hence $h \in A_{d+\deg(u)}$ again. So we have to verify that $(U^{-1}A)_d$ is an R-sub-module. Suppose $a \in R$ and g/u, $h/v \in (U^{-1}A)_d$. Then $ag \in A_{d+\deg(u)}$ and hence $a(g/u) \in (U^{-1}A)_d$ again. Furthermore

$$\frac{g}{u} + \frac{h}{v} \;=\; \frac{gv + hu}{uv}$$

As $\deg(uv) = \deg(u) + \deg(v)$ we have gv and $hu \in A_{d+\deg(uv)}$ thus $gv + hv \in A_{d+\deg(uv)}$ again and this means $(gv + hu)/uv \in (U^{-1}A)_d$. So let us now verify property (4) of graded algebras. To do this consider $g/u \in (U^{-1}A)_c$ and $h/v \in (U^{-1}A)_d$. Then we have to verify $(gh)/(uv) = (g/u)(h/v) \in (U^{-1}A)_{c+d}$. If $(gh)/(uv) = 0$ we are done, else we have $\deg(g) = c + \deg(u)$ and $\deg(h) = d + \deg(v)$. Thus $\deg(gh) = \deg(g) + \deg(h) = c + \deg(u) + d + \deg(v) = (c+d) + \deg(uv)$. And this already is $(gh/(uv) \in (U^{-1}A)_{c+d}$. It remains to verify property (3) of graded algebras. Given any $f/u \in U^{-1}A$ let us pick up a homogeneous decomposition $f = \sum_d f_d$ of f in A. Then $f/u = \sum_d f_d/u$ and as $f_d/u \in (U^{-1}A)_{d-\deg(u)}$ and as f has been arbitrary this means $U^{-1}A = \sum_d (U^{-1}A)_d$. Thus it only remains to prove

$$\Big(U^{-1}A\Big)_d \cap \left(\sum_{c \neq d} \Big(U^{-1}A\Big)_c\right) \;=\; 0$$

Thus consider some h/v contained in the intersection. We have to prove $h/v = 0/1$ thus let us suppose $h/v \neq 0/1$ and deduce a contradiction. As $h/v \in (U^{-1}A)_d$ that is $h \in A_{d+\deg(v)}$. And likewise there is some finite subset $\Omega \subseteq D \setminus \{c\}$ and $u_c \in U$, $g_c \in A_{c+\deg(u_c)}$ (where $c \in \Omega$) such that $h/v = \sum_c g_c/u_c$. Now let $u := \prod_c u_c \in U$ and $\widehat{u}_c := u/u_c \in U$ then we compute

$$\frac{h}{v} \;=\; \sum c \in \Omega \frac{g_c}{u_c} \;=\; \frac{1}{u}\left(\sum_{c\in\Omega} g_c \widehat{u}_c\right)$$

That is there is some $w \in U$ such that $uwh = vw\sum_c g_c\widehat{u}_c$. Note that uwh and the $vwg_c\widehat{u}_c$ are homogeneous elements of A, where

$$\begin{aligned}
\deg(vwg_c\widehat{u}_c) &= \deg(v) + \deg(w) + c + \deg(u_c) + \sum_{b\neq c} \deg(u_b) \\
&= \deg(v) + \deg(w) + c + \sum_{c\in\Omega} \deg(u_c) \\
&= \deg(uvw) + c
\end{aligned}$$

Hence all the $vwg_c\widehat{u}_c$ have different degrees and hence form a homogeneous decomposition of uwh. This however is homogeneous too, of degree $\deg(uwh) = \deg(uw) + d + \deg(v) = \deg(uvw) + d$. As $c \neq d$ this is yet another homogeneous decomposition. Hence $uwh = 0$ which would mean $h/v = 0/1$, a contradiction.

(v) Consider any $f \in \sqrt{\mathfrak{a}}$ that is $f^k \in \mathfrak{a}$ for some $k \in \mathbb{N}$. If $k = 0$ then $1 \in \mathfrak{a}$ and hence $\mathfrak{a} = A$. This would imply $\sqrt{\mathfrak{a}} = A$, too, which clearly is a graded ideal again. Thus let us consider the case $k \geq 1$. Pick up the hoomogeneous decomposition $f = \sum_d f_d$ of f, then by (7.46) it suffices to check

$f_d \in \sqrt{\mathfrak{a}}$ for any $d \in \mathbb{N}$. Now compute

$$f^k \;=\; \sum_{\alpha\in\mathbb{N}^k} f_{\alpha_1}\dots f_{\alpha_k} \;=\; \sum_{d\in\mathbb{N}}\sum_{|\alpha|=d} f_{\alpha_1}\dots f_{\alpha_k} \;\in\; \mathfrak{a}$$

where $|\alpha| := \alpha_1 + \dots + \alpha_k \in \mathbb{N}$. By definition of graded algebras it is clear that $f_{\alpha_1}\dots f_{\alpha_k} \in A_{|\alpha|}$ and thus we have found the homogeneous decomposition of f^k. As $\mathfrak{a}$ is a graded ideal, this implies

$$\forall\, d \in \mathbb{N} \;:\; \sum_{|\alpha|=d} f_{\alpha_1}\dots f_{\alpha_k} \;\in\; \mathfrak{a}$$

We will now prove that $f_d \in \sqrt{\mathfrak{a}}$ by induction on d. For $d = 0$ we have $\{\, |\alpha| = 0 \,\} = \{0\}$ and hence $f_0^k = \sum_{|\alpha|=0} f_{\alpha_1}\dots f_{\alpha_k} \in \mathfrak{a}$. Thus suppose $d \geq 1$, then we define the following function

$$\mu \;:\; \{\, |\alpha| = kd \,\} \to \mathbb{N} \;:\; \alpha \mapsto \min\{\, \alpha_i \mid i \in 1\dots k \,\}$$

It is clear that $\mu(\alpha) \leq d$ (as else $|\alpha| \geq k(d+1) > kd$) and that $\mu(\alpha) = d$ is equivalent to $\alpha = (d,\dots,d)$ (as else $|\alpha| > kd$). Hence we get

$$\begin{aligned} f_d^k &= \sum_{\mu(\alpha)=d} f_{\alpha_1}\dots f_{\alpha_k} \\ &= \sum_{|\alpha|=kd} f_{\alpha_1}\dots f_{\alpha_k} - \sum_{\mu(\alpha)<d} f_{\alpha_1}\dots f_{\alpha_k} \end{aligned}$$

But we have already seen from the gradedness of $\mathfrak{a}$ that the first term (the sum over $|\alpha| = kd$) is contained in $\mathfrak{a}$ again. And if $\mu(\alpha) < d$ then the induction hypothesis yields $f_{\mu(\alpha)} \in \sqrt{\mathfrak{a}}$. Yet it is clear that $f_{\mu(\alpha)} \mid f_{\alpha_1}\dots f_{\alpha_k}$ and hence $f_{\alpha_1}\dots f_{\alpha_k} \in \sqrt{\mathfrak{a}}$ again. Thus the second term (the sum over $\mu(\alpha) < d$) is contained in $\sqrt{\mathfrak{a}}$, too. And this implies $f_d^k \in \sqrt{\mathfrak{a}}$ and hence even $f_d \in \sqrt{\mathfrak{a}}$, which had to be shown.

□

Proof of (7.42):
The only statements that is not covered in (6.41) is the fact that the multiplication $R^2 \to R : (a,b) \mapsto ab$ is continuous, as well. And for this we also have to prove the explicit reformulation in terms of the box topology, given in the note. By definition the multiplication is continuous, iff for any open set $W \subseteq R$ the preimage $P := \{\, (a,b) \in R^2 \mid ab \in W \,\}$ is an open set in R^2. But by definition of the box topology P is open, iff for any $(a,b) \in P$ there are open subsets $U \in \mathcal{O}(a)$ and $V \in \mathcal{O}(b)$ such that $U \times V \subseteq P$. The latter means $uv \in W$ for any $u \in U$ and $v \in V$ and likewise $(a,b) \in P$ translates into $ab \in W$.
That is, we have to verify: For any a, $b \in R$ with $ab \in W$ there are some $U \in \mathcal{O}(a)$ and $V \in \mathcal{O}(b)$ such that for any $u \in U$ and any $v \in V$ we have $uv \in W$ again. So we start with a, $b \in R$ such that $ab \in W$ and have to find these open neighbourhoods U and V. As $W \subseteq R$ is open, there is some $n \in \mathbb{N}$ such that $ab + \mathfrak{a}^n \subseteq W$. We then choose $U := B_r(a)$ and $V := B_r(b)$ for $r := 2^{-n}$. That is $u \in U$ means $d(a,u) < r$ which turns into $\operatorname{ord}(u-a) > n$. In particular $\alpha := u - a \in \mathfrak{a}^n$ (even in $\mathfrak{a}^{n+1}$, but we do not need this). Likewise $\beta := v - b \in \mathfrak{a}^n$ and therefore $uv = (a+\alpha)(b+\beta) = ab + \alpha b + a\beta + \alpha\beta \in ab + \mathfrak{a}^n \subseteq W$. That is we have found $uv \in W$ again, as required. □

Proof of (7.44):

We begin by verifying, that $R_{\mathfrak{a}}[t]$ truly is a sub-algebra of $R[t]$: It is clear, that $R_{\mathfrak{a}}[t]$ is an additive subgroup of $R[t]$ and that $\mathbf{1} \in R_{\mathfrak{a}}[t]$. The only not trivial part is that $R_{\mathfrak{a}}[t]$ is closed under multiplication. So consider any two $f, g \in R_{\mathfrak{a}}[t]$, then for any $n \in \mathbb{N}$ we have

$$(fg)[n] \;=\; \sum_{i=0}^{n} f[i]\, g[n-i] \;\in\; \sum_{i=0}^{n} \mathfrak{a}^i\, \mathfrak{a}^{n-i} \;=\; \mathfrak{a}^n$$

such that $fg \in R_{\mathfrak{a}}[t]$ again. And from this we also see, that ϱ is a homomorphism of rings. It also is clear from the construction of the Rees-algebra, that ϱ is surjective, as the n-th component of $(f_n + \mathfrak{a}^{n+1}) \in R(\mathfrak{a})$ is contained in $f_n \in \mathfrak{a}^n$. It also is clear, that $\varrho(g) = 0$ is equivalent, to

$$g \;\in\; \left\{ f \in R[t] \mid \forall\, n \in \mathbb{N} : f[n] \in \mathfrak{a}^{n+1} \right\}$$

so let us argue, that this truly is the ideal generated, by $\{\, a\mathbf{1} \mid a \in \mathfrak{a} \,\} \subseteq R_{\mathfrak{a}}[t]$. By construction the elements of this ideal are of the form $f = a_1 f_1 + \cdots + a_k f_k$ where $a_i \in \mathfrak{a}$ and $f_i \in R_{\mathfrak{a}}[t]$. Let us evaluate what this means

$$f[n] \;=\; \sum_{n=0}^{\infty} \left(a_1 f_1[n] + \ldots a_k f_k[n] \right)$$

As $f_i[n] \in \mathfrak{a}^n$ and $a_i \in \mathfrak{a}$ by assumption, this means $f[n] \in \mathfrak{a}^{n+1}$ and hence f is in the kernel of ϱ. And the same is true in the opposite direction: If $\varrho(f) = 0$, then $f[n] \in \mathfrak{a}^{n+1} = \mathfrak{a}\,\mathfrak{a}^n$. And thereby the product $\mathfrak{a}\,\mathfrak{a}^n$ contains elements of the form $a_1 b_1 + \cdots + a_k b_k$, where $a_i \in \mathfrak{a}$ and $b_i \in \mathfrak{a}^n$. As $f \in R[t]$ it is of finite degree and any $k(n)$ is finite, we find that f is a finite sum of terms of the form $a_i b_i t^n$, for some $a_i \in \mathfrak{a}$ and $b_i \in \mathfrak{a}^n$. But such sums are contained in the ideal generated by $\{\, a\mathbf{1} \mid a \in \mathfrak{a} \,\}$ in $R_{\mathfrak{a}}[t]$. □

Proof of (7.51):

(i) If $h \in A_d$ but $h \neq 0$ then the homogeneous decomposition $h = \sum_c h_c$ has precisely one non-zero entry $h = h_d$ at $c = d$ (by comparing coefficients). Thus $\deg(h) = \max\{\, d \,\}$ and this clearly is d.

(ii) If $f \in A_{\text{hom}}$ with $f \in A_d$ then we have just argued in (i) that $\deg(f) = \max\{\, d \,\} = d$. And likewise $\operatorname{ord}(f) = \min\{\, d \,\} = d$ which yields $\operatorname{ord}(f) = \deg(f)$. Conversely suppose $d := \operatorname{ord}(f) = \deg(f)$, then we use a homogeneous decomposition $f = \sum_c f_c$ again. By construction, if $c < d = \operatorname{ord}(f)$ or $d = \deg(d) < c$ then $f_c = 0$. Thus it only remains $f = f_d \in A_d$ and hence $f \in hogA$.

(iii) As $\operatorname{ord}(f)$ is the minimum and $\deg(f)$ is the maximum over the common set $\{\, d \in D \mid f_d \neq 0 \,\}$ it is clear, that $\operatorname{ord}(f) \leq \deg(f)$. Now let $a := \deg(f)$ and $b := \deg(g)$. Then (by construction of the degree) the homogeneous decompositions of f and g are of the form

$$f = \sum_{c \leq a} f_c \quad \text{and} \quad g = \sum_{d \leq b} g_d$$

Thus the product fg is given by a sum over two indexes $c \leq a$ and $d \leq b$. Assorting the (c,d) according to the sum $c + d$ we find that

$$fg \;=\; \left(\sum_{c \leq a} f_c \right) \left(\sum_{d \leq b} g_d \right) \;=\; \sum_{c \leq a} \sum_{d \leq b} f_c g_d \;=\; \sum_{e \in D} \sum_{c+d=e} f_c g_d$$

Note that thereby $f_c g_d \in A_{c+d} = A_e$. Thus we have found the homogeneous decomposition of fg again. But as D was assumed to be positive $c \leq a$ and $d \leq b$ implies $e = c + d \leq a + d \leq a + b$. Thus the homogeneous decomposition is of the following form

$$fg \;=\; \sum_{e \leq a+b} \left(\sum_{c+d=e} f_c g_d \right)$$

And this of course means $\deg(fg) \leq a + b = \deg(f) + \deg(g)$. The claim for the order can be shown in complete analogy. Just let $a := \operatorname{ord}(f)$ and $b := \operatorname{ord}(g)$. Then f and g can be written as

$$f = \sum_{c \geq a} f_c \quad \text{and} \quad g = \sum_{d \geq b} g_d$$

Thus in complete analogy to the above one finds that the homogeneous decomposition of fg is of the following form (which already yields $\operatorname{ord}(fg) \geq a + b = \operatorname{ord}(f) + \operatorname{ord}(g)$)

$$fg \;=\; \sum_{e \geq a+b} \left(\sum_{c+d=e} f_c g_d \right)$$

(iv) We commence with the proof given in (iii), that is $a = \deg(f)$ and $b = \deg(g)$. In particular $f_a \neq 0$ and $g_b \neq 0$. But as A is now assumed to be an integral domain this yields $f_a g_b \neq 0$. We have already found the homogeneous decomposition of fg to be

$$fg \;=\; \sum_{e \leq a+b} \left(\sum_{c+d=e} f_c g_d \right)$$

So let us take a look at the homogeneous component $(fg)_{a+b}$ of degree $a + b \in D$. Given any $c \leq a$ and $d \leq b$ we get the implication

$$c + d = a + b \quad \Longrightarrow \quad (c, d) = (a, b)$$

Because if we had $c \neq a$ then $c < a$ and hence $c + d < a + d \leq a + b$, as D was assumed to be strictly positive. Likewise $d \neq b$ would imply $c + d < a + b$ in contradiction to $c + d = a + b$. Thus the homogeneous component $(fg)_{a+b}$ is given to be

$$(fg)_{a+b} \;=\; \sum_{c+d=a+b} f_c g_d \;=\; f_a g_b \;\neq\; 0$$

In particular we find $\deg(fg) \geq a + b = \deg(f) + \deg(g)$ and hence $\deg(fg) = \deg(f) + \deg(g)$. By replacing the above implication with $c \geq a$, $d \geq b$ and $c + d = a + b$ implies $(c, d) = (a, b)$ the claim for the order $\operatorname{ord}(fg) = \operatorname{ord}(f) + \operatorname{ord}(g)$ can be proved in complete analogy.

(v) As D is strictly positive it already is integral, according to (7.6.(iii)). Hence by (7.48.(i)) we already know $1 \in A_0$ and hence $\deg(1) = 0$ according to (i). And as 1 is homogeneous we also get $\operatorname{ord}(1) = \deg(1) = 0$, according to (ii). Now suppose $f \in A^*$ is an invertible element of A. Then

we use (iv) to compute

$$0 \;=\; \deg(1) \;=\; \deg(ff^{-1}) \;=\; \deg(f)+\deg(f^{-1})$$

$$0 \;=\; \operatorname{ord}(1) \;=\; \operatorname{ord}(ff^{-1}) \;=\; \operatorname{ord}(f)+\operatorname{ord}(f^{-1})$$

And as $\operatorname{ord}(f) \leq \deg(f)$ and $\operatorname{ord}(f^{-1}) \leq \deg(f^{-1})$ (due to (iii)) the positivity of D can be used to find the following estimates

$$\begin{aligned} 0 \;&=\; \operatorname{ord}(f)+\operatorname{ord}(f^{-1}) \;\leq\; \deg(f)+\operatorname{ord}(f^{-1}) \\ &\leq\; \deg(f)+\deg(f^{-1}) \;=\; 0 \end{aligned}$$

In particular we find $\operatorname{ord}(f)+\operatorname{ord}(f^{-1}) = \deg(f)+\operatorname{ord}(f^{-1})$. Adding $\operatorname{ord}(f)$ this equation turns into $\operatorname{ord}(f) = \deg(f)$ and by (ii) again this means that $f \in hogA$ is homogeneous.

(vi) Let us suppose $h = fg$ for some $g \in A$. As $h \in hogA$ we have $h \neq 0$ and this also implies $f, g \neq 0$. We will assume that f was *not* homogeneous and derive a contradiction. Recall that by (iii) f not being homogeneous is equivalent to $\operatorname{ord}(f) < \deg(f)$. But if that was true we could use (iv) to find the contradiction

$$\begin{aligned} \operatorname{ord}(h) \;&=\; \operatorname{ord}(fg) \;=\; \operatorname{ord}(f)+\operatorname{ord}(g) \\ &<\; \deg(f)+\operatorname{ord}(g) \;\leq\; \deg(f)+\deg(g) \\ &=\; \deg(fg) \;=\; \deg(h) \;=\; \operatorname{ord}(h) \end{aligned}$$

□

Proof of (7.12):

(i) Consider any $b \in R$ and any polynomial $f \in R[t \mid A]$. Then for any $\gamma \in A$ we get the following computation

$$(f \cdot bt^0)[\gamma] \;=\; \sum_{\alpha+\beta=\gamma} f[\alpha]\, bt^0[\beta] \;=\; \sum_{\alpha+\beta=\gamma} f[\alpha]\, b\delta_{\beta,\gamma} \;=\; bf[\gamma]$$

In complete analogy we see, that $(bt^0 \cdot f)[\gamma] = bf[\gamma]$. And as this is true for any $\gamma \in A$ we have shown $f \cdot bt^0 = bf$ and $bt^0 \cdot f = bf$. In particular for $b = 1$ we get $f \cdot t^0 = f = t^0 \cdot f$. That is t^0 is the unit element of the ring $R[t \mid A]$ or shortly $t^0 = \mathbf{1}$.

(ii) In the proof of (i) (by taking $f = at^0$ for some $a \in R$) we have seen, that $(at^0) \cdot (bt^0) = (ab)t^0$ such that ι is multiplicative. And the additivity of ι is clear by construction of $R[t \mid A]$. But the injectivity of ι is trivial, as well.

(iii) Given $f \in R[\![t \mid A]\!]$ let us define $\iota(f) \in R[\![t \mid B]\!]$ to be $\iota(f)[\alpha] := f[\alpha]$ for $\alpha \in A$ and $\iota(f)[\beta] := 0$ for $\beta \in B \setminus A$. Then clearly $f \mapsto \iota(f)$ is injective and R-linear. Also $\iota(\mathbf{1}) = \mathbf{1}$, as $0 \in A$. It remains

to check the multiplicativity of ι: Consider any $\gamma \in B$, then

$$\big(\iota(f)\cdot\iota(g)\big)[\gamma] \;=\; \sum_{\alpha+\beta=\gamma} \begin{cases} f[\alpha] \text{ if } \alpha \in A \\ \quad 0 \text{ if } \alpha \notin A \end{cases} \begin{cases} g[\beta] \text{ if } \beta \in A \\ \quad 0 \text{ if } \beta \notin A \end{cases}$$

where the sum runs over all α and $\beta \in B$ with $\alpha+\beta=\gamma$. Yet all the summands vanish, unless $\alpha \in A$ and $\beta \in A$. And as A is a submonoid this also implies $\gamma = \alpha+\beta \in A$. Thus this is precisely $(f\cdot g)[\gamma]$ for $\gamma \in A$ and 0 if $\gamma \notin A$. Thus we find the multiplicativity

$$\big(\iota(f)\cdot\iota(g)\big)[\gamma] \;=\; \iota\big(f\cdot g\big)[\gamma]$$

(iv) The fact that $\overline{\varphi} : R[t \mid A] \to S[t \mid A]$ is a homomorphism of R-algebras is just a special case of (7.14) if we take $\sigma : A \to S[t \mid A]$ to be $\sigma(\alpha) := t^\alpha$. In case of the ring of formal power series $S[\![t \mid A]\!]$ the computations are literally the same.

Thus let us suppose φ is injective and $\overline{\varphi}(f) = \overline{\varphi}(g)$ for some $f, g \in R[\![t \mid A]\!]$. By definition of formal power series, this is $\overline{\varphi}(f)[\alpha] = \overline{\varphi}(g)[\alpha]$ for any $\alpha \in A$. And by construction this is $\varphi(f[\alpha]) = \varphi(g[\alpha])$. But as φ this implies $f[\alpha] = g[\alpha]$ for any $\alpha \in A$ and hence $f = g$. Thus $\overline{\varphi}$ also is injective.

And if φ is surjective and we are given any $g \in S[\![t \mid A]\!]$ then for any α we may choose $f[\alpha] \in R$ such that $\varphi(f[\alpha]) = g[\alpha]$. Then by construction we have $\overline{\varphi}(f) = g$ such that $\overline{\varphi}$ is surjective. In particular if φ is bijective then φ is both, injective and surjective and this is true for $\overline{\varphi}$, as well.

(v) Is obvious by the multiplicative property $t^\alpha\, t^\beta = t^{\alpha+\beta}$ of monomials, which has been shown in the remark preceding this proposition.

(vi) Let us first suppose A and B are solution-finite and consider any $a \in R$ and $f, g \in R[\![s \mid A]\!][\![t \mid B]\!]$. By construction we have $f[\beta] \in R[\![s \mid A]\!]$ for any $\beta \in B$. That is f is of the form

$$f \;=\; \sum_{\beta\in B} f[\beta]\, t^\beta \;=\; \sum_{\beta\in B} \left(\sum_{\alpha\in A} f[\beta]f[\alpha]\, s^\alpha \right) t^\beta$$

We have defined the isomorphism Φ by $\Phi(f) : (\alpha,\beta) \mapsto f[\beta]f[\alpha]$. In particular it is clear that Φ is bijective, as it only rearranges coefficients. So it only remains to prove its homomorphism properties: First of all it is clear, that Φ is additive, since

$$\begin{aligned} \Phi(f+g)[\alpha,\beta] &= (f+g)[\beta][\alpha] \\ &= \big(f[\beta]+g[\beta]\big)[\alpha] \\ &= f[\beta][\alpha] + g[\beta][\alpha] \\ &= \Phi(f)[\alpha,\beta] + \Phi(g)[\alpha,\beta] \end{aligned}$$

As A and B are solution-finite, so is $A \times B$, by (7.2). Therefore all the R-modules of formal power series involved are R-algebras. The R-linearity will then be a special case of the multiplicativity of Φ that we will prove next: Let $\alpha, \gamma, \varepsilon \in A$ and $\beta, \delta, \eta \in B$, then we get

$$\Phi(f\cdot g)[\varepsilon,\eta] \;=\; (f\cdot g)[\eta][\varepsilon]$$

$$
\begin{aligned}
&= \left(\sum_{\beta+\delta=\eta} f[\beta] \cdot g[\alpha] \right) [\varepsilon] \\
&= \sum_{\alpha+\gamma=\varepsilon} \sum_{\beta+\delta=\eta} f[\beta][\alpha] \cdot g[\alpha][\gamma] \\
&= \sum_{(\alpha,\beta)+(\gamma,\delta)=(\varepsilon,\eta)} f[\beta][\alpha] \cdot g[\alpha][\gamma]
\end{aligned}
$$

On the other hand, if we take a look at $\Phi(f) \cdot \Phi(g)$, then we find the multiplicativity $\Phi(f \cdot g) = \Phi(f) \cdot \Phi(g)$ as the left and right-hand side expressions agree in every coefficient over (ε, η)

$$
\begin{aligned}
\big(\Phi(f) \cdot \Phi(g)\big)[\varepsilon,\eta] &= \sum_{(\alpha,\beta)+(\gamma,\delta)=(\varepsilon,\eta)} \Phi(f)[\alpha,\beta] \cdot \Phi(g)[\gamma,\delta] \\
&= \sum_{(\alpha,\beta)+(\gamma,\delta)=(\varepsilon,\eta)} f[\beta][\alpha] \cdot g[\alpha][\gamma] \\
&= \Phi(f \cdot g)[\varepsilon,\eta]
\end{aligned}
$$

That is we have proved the isomorphy of the R-algebras $R[\![s \mid A]\!][\![t \mid B]\!]$ and $R[\![x \mid A \times B]\!]$. It is clear that Φ maps polynomials to polynomials: As Φ only rearranges the coefficients it does not change the number of non-zero entries. Therefore Φ is an isomorphism from $R[s \mid A][t \mid B]$ to $R[x \mid A \times B]$. And as the homomorphism property remains, even if A or B is not solution-finite, this is true for general A and B.

(vii) Let us first consider the case that R is an integral domain: We choose any two non-zero polynomials $0 \neq f, g \in R[t \mid A]$ and denote the coefficients on which f and g are non-zero by

$$
\begin{aligned}
\{\, \alpha_1, \ldots, \alpha_m \,\} &:= \{\, \alpha \in A \mid f[\alpha] \neq 0 \,\} \\
\{\, \beta_1, \ldots, \beta_n \,\} &:= \{\, \beta \in A \mid g[\beta] \neq 0 \,\}
\end{aligned}
$$

Without loss of generality we may assume $\alpha_1 < \cdots < \alpha_m$ and likewise $\beta_1 < \cdots < \beta_n$. Let us now abbreviate $\gamma := \alpha_1 + \beta_1$, then for any $i \in 1 \ldots m$ and $j \in 1 \ldots n$ proposition (7.6.(iv)) implies

$$
\alpha_i + \beta_j = \gamma \implies \alpha_i = \alpha_1 \text{ and } \beta_i = \beta_1
$$

We now assume $fg = 0$ and use the above implication to compute the γ-coefficient of fg, obtaining

$$
0 = (f\,g)[\gamma] = \sum_{\alpha_i+\beta_j=\gamma} f[\alpha_i]\, g[\beta_j] = f[\alpha_1]\, g[\beta_1]
$$

If now R is integral then $f[\alpha_1] = 0$ or $g[\beta_1] = 0$ in contradiction to the construction $f[\alpha_1]$ and $g[\beta_1] \neq 0$. But this ensures the direction (a) $\implies$ (b). The converse implication is clear due to the embedding $R \hookrightarrow R[t \mid A]$ in (ii) however.

(vii) Let us now prove that $R[t \mid A]$ is reduced, whenever R is reduced. That is we consider some polynomial $g \in R[t \mid A]$ such that $g^r = 0$ for some $r \in \mathbb{N}$ and have to prove $g = 0$. Let us start with $g \neq 0$, then we have to falsify the assumption $g^r = 0$. To do this let $\{\, \beta_1, \ldots, \beta_n \,\}$ be the set of $\beta \in A$ such that $g[\beta] \neq 0$ again. As before we may assume $\beta_1 < \cdots < \beta_n$. Then the polynomial

rule (1.41) tells us

$$g^r \;=\; \left(\sum_{j=1}^{n} g[\beta_j]\, t^{\beta_j}\right)^r \;=\; \sum_{|\alpha|=r} \binom{r}{\alpha} \prod_{j=1}^{r} \left(g[\beta_j]\, t^{\beta_j}\right)^{\alpha_j} \;=\; \sum_{|\alpha|=r} \binom{r}{\alpha} \left(\prod_{j=1}^{r} g[\beta_j]^{\alpha_j}\right) t^{\langle\alpha|\beta\rangle}$$

where the sum runs over all $\alpha \in \mathbb{N}^n$ such that $\alpha_1 + \cdots + \alpha_n = r$. In the last sum we denoted $\langle \alpha \mid \beta \rangle := \alpha_1\beta_1 + \cdots + \alpha_n\beta_n \in A$. It is clear that among all these α precisely $\alpha = (r, 0, \ldots, 0)$ yields the minimal $\langle \alpha \mid \beta \rangle = r\beta_1$. All the other α yield $r\beta_1 < \langle \alpha \mid \beta \rangle$ such that

$$g^r[r\beta_1] \;=\; g[\beta_1]^r$$

as for this $\alpha = (r, 0, \ldots, 0)$ the binomial coefficient is 1. Now, if we had $g^r = 0$ then this would imply $g[\beta_1]^r = 0$ and as R is reduced, this would imply $g[\beta_1] = 0$ in contradiction to our construction $g[\beta_1] \neq 0$. Thus we have falsified $g^r = 0$ and hence the implication (a) $\implies$ (b). The converse implication is clear due to the embedding $R \hookrightarrow R[t \mid A]$ in (ii) again.

(viii) First of all note that the assumption $L_\gamma := \{\, \alpha \in A \mid \alpha \leq \gamma \,\}$ being a finite set for any $\gamma \in A$ implies A to be solution-finite, by (7.6.(viii)) and hence $R[\![t \mid A]\!]$ is an R-algebra. Now consider any $f \in R[\![t \mid A]\!]$, then we can define

$$\operatorname{ord}(f) \;:=\; \min\{\, \alpha \in A \mid f[\alpha] \neq 0 \,\}$$

This is due to the following reasoning: Choose any $\gamma \in A$ with $f[\gamma] \neq 0$, then the set of all non-zero coefficients of f up to γ is $\{\, \alpha \in A \mid \alpha \leq \gamma \text{ and } f[\alpha] \neq 0 \,\} \subseteq L_\gamma$ a finite set. Let $\mu \in A$ be the minimum of this set. If now $\alpha \in A$ is any element with $f[\alpha] \neq 0$, then we distinguish two cases: If $\alpha \leq \gamma$, then we have $\mu \leq \alpha$ by minimality of μ. And if $\alpha > \gamma$ then $\mu \leq \gamma < \alpha$ also implies $\mu \leq \alpha$. Thus we have $\mu \leq \alpha$ for any α with $f[\alpha] \neq 0$, which means $\operatorname{ord}(f) = \mu$ exists.

Now if we are given any two formal power seires $f, g \in R[\![t \mid A]\!]$ with $f, g \neq 0$ let $\alpha_1 := \operatorname{ord}(f)$ and $\beta_1 := \operatorname{ord}(g)$. Then we can proceed as in (vii) above: If $\gamma := \alpha_1 + \beta_1$ then for any $\alpha, \beta \in A$ with $f[\alpha] \neq 0$ and $g[\beta] \neq 0$ we get

$$\alpha + \beta \;=\; \gamma \quad\Longrightarrow\quad \alpha \;=\; \alpha_1 \;\text{ and }\; \beta \;=\; \beta_1$$

by (7.6.(iv)) again. Thus we get $fg[\gamma] = f[\alpha_1]g[\beta_1]$ as before. Now if R is an integral domain and $fg = 0$ then this would imply $f[\alpha_1] = 0$ or $g[\beta_1] = 0$ a contradiction to $f \neq 0$ and $g \neq 0$. Thus $R[\![t \mid A]\!]$ is an integral domain, again.

In particular, we see by induction on r, that $f[r\alpha_1] = f[\alpha_1]^r$. Thus if R is reduced and $f^r = 0$ then we conclude $f[\alpha_1]^r = 0$ which turns into $f[\alpha_1] = 0$, a contradiction again. Thus if we start with a reduced ring R, then $R[\![t \mid A]\!]$ will be reduced, again. The converse implications are clear due to the embeddings $R \hookrightarrow R[t \mid A]$ in (ii) and $R[t \mid A] \hookrightarrow R[\![t \mid A]\!]$ by (iii).

□

Proof of (7.14):

It is obvious that the ring homomorphism σ_φ is uniquely determined by the above properties, as the monomials t^α form a basis of $R[t \mid A]$ and the compositions $+$ and $\cdot$ are expanded from the monomials. Thus

it only remains to show that σ_φ truly is a ring-homomorphism, but this is a straightforward computation - consider $f,g \in R[t \mid A]$, then we find

$$\begin{aligned}\sigma_\varphi(f)+\sigma_\varphi(g) &= \sum_{\alpha\in A}\varphi(f[\alpha])\,\sigma(\alpha) \;+\; \sum_{\alpha\in A}\varphi(g[\alpha])\,\sigma(\alpha)\\ &= \sum_{\alpha\in A}\varphi\big(f[\alpha]+g[\alpha]\big)\,\sigma(\alpha)\\ &= \sigma_\varphi(f+g)\end{aligned}$$

$$\begin{aligned}\sigma_\varphi(f)\cdot\sigma_\varphi(g) &= \left(\sum_{\alpha\in A}\varphi(f[\alpha])\,\sigma(\alpha)\right)\;\cdot\;\left(\sum_{\beta\in A}\varphi(g[\beta])\,\sigma(\beta)\right)\\ &= \sum_{\alpha\in A}\sum_{\beta\in A}\varphi\big(f[\alpha]\cdot g[\beta]\big)\,\sigma(\alpha+\beta)\\ &= \sum_{\gamma\in A}\varphi\left(\sum_{\alpha+\beta=\gamma} f[\alpha]\cdot g[\beta]\right)\sigma(\gamma)\\ &= \sigma_\varphi(fg)\end{aligned}$$

$$\begin{aligned}\sigma_\varphi(af) &= \left(\sum_{\alpha\in A}\varphi(af[\alpha])\,\sigma(\alpha)\right)\\ &= \sum_{\alpha\in A}\varphi(a)\cdot\varphi(f[\alpha])\,\sigma(\alpha)\\ &= \varphi(a)\cdot\sum_{\alpha\in A}\varphi(f[\alpha])\,\sigma(\alpha)\\ &= \varphi(a)\cdot\sigma_\varphi(f)\end{aligned}$$

□

Proof of (7.16):
Let $I := R\setminus\{\,0_R,1_R\,\}$ where 0_R and 1_R denote the zero resp. the unit element of R. Further let $A := \mathbb{N}^{\oplus I}$ be the commutative monoid over the index set I. Now take the polynomial ring

$$S \;:=\; \mathbb{Z}[t_a \mid a\in I]$$

As A can be turned into a positively ordered monoid $(A,+,\leq_{\text{lex}})$ according to (7.8) and $\mathbb{Z}$ is an integral domain, so is S due to proposition (7.12.(iv)). And clearly $\zeta : \mathbb{Z}\to R : k\mapsto k\cdot 1_R$ is a well-defined homomorphism of rings (which we used in section 2.9 to introduce the characteristic). And there is a well-defined homomorphism of monoids $\alpha : A\to R$, induced by expansion of $\zeta(\delta_a)=a$. By (7.14) we now find a well-defined homorphsim of rings $\varrho := \alpha_\zeta : S\to R$. And this ϱ clearly is surjective, since $\varrho(t_a)=a$. □

Proof of (7.54):

(i) The proof is based on a computation in which we evaluate $g(t) := f(t)\cdot(t-a)$. By definition of

the multiplication in $R[t]$ this is nothing but

$$\begin{aligned}\sum_{k=0}^{\infty} g[k]t^k &= \left(\sum_{k=0}^{\infty} f[k]t^k\right)(t-a)\\ &= \sum_{k=0}^{\infty} f[k]t^{k+1} - \sum_{k=0}^{\infty} af[k]t^k\\ &= \sum_{k=1}^{\infty} \big(f[k-1] - af[k]\big)\, t^k - af[0]\end{aligned}$$

So by comparing coefficients we find $g[0] = -af[0]$ and for any $k \geq 1$ also $g[k] = f[k-1] - af[k]$. Let us first deal with (b) $\implies$ (a): That is we assume that $\deg(f) = n-1$ and $f[n-1] = 1$. More explicitly for any $k \geq n$ we have $f[k] = 0$. Then for any $k > n$ we find that

$$\begin{aligned}g[n] &= f[n-1] - af[n] \;=\; 1 - a\cdot 0 \;=\; 1\\ g[k] &= f[k-1] - af[k] \;=\; 0 - a\cdot 0 \;=\; 0\end{aligned}$$

That is g is a monic polynomial of degree n, as we had claimed. Conversely for (a) $\implies$ (b) we have $g[n] = 1$ and $g[k] = 0$ for any $k > n$. Clearly $f \neq 0$, as else $g = 0$ which contradicts g being monic, as $R \neq 0$. Hence we may take $m := \deg(f) \in \mathbb{N}$. As $f[m+1] = 0$ we then get

$$g[m+1] \;=\; f[m] - af[m+1] \;=\; f[m] - a\cdot 0 \;=\; f[m] \;\neq\; 0$$

From this we conclude $\deg(g) \geq m+1 > \deg(f)$. And for any $k > m+1$ we have $k-1 > m$ and hence $f[k-1] = 0$ and $f[k] = 0$ such that we also find $\deg(g) \leq m+1$ from

$$g[k] \;=\; f[k-1] - af[k] \;=\; 0 - a\cdot 0 \;=\; 0$$

Together this means $n = \deg(g) = m+1$ such that $\deg(f) = m = n-1$. But g is monic such that $1 = g[n] = g[m+1] = f[m]$ which means, that f is monic, too. Together this is (b), as claimed.

(ii) Let us use division with remainder (2.67) to divide f by $t-a$ (which is possible, as $t-a$ is monic). That is we find polynomials q, $r \in R[t]$ such that $r = 0$ or $\deg(r) < \deg(t-a)$ and

$$f(t) \;=\; q(t)\cdot(t-a) + r(t)$$

If $r = 0$, then $r \in R$. But also $\deg(r) < \deg(t-a) = 1$ implies $\deg(r) = 0$, which is $r \in R$ again. In other words $r(t) = r$ is a constant. Let us now use (7.14) in the standard situation $S = R$, $\varphi = \mathbb{1}$ and $\sigma(k) = a^k$. As $\sigma_{\mathbb{1}}$ is a homomorphism or rings we get - for $f(a) := \sigma_{\mathbb{1}}(f)$

$$f(a) \;=\; q(a)\cdot(a-a) + r(a) \;=\; r(a)$$

But as $r(t) = r$ is a constant we have $r(a) = \mathbb{1}(r) = r$, as well. Hence the above representation $f(t) = q(t)(t-a) + r(t)$ turns into $f(t) = q(t)(t-a) + f(a)$, which is our claim precisely.

(iii) In the direction " $\implies$ " we use (ii) to write f as $f(t) = q(t)(t-a) + f(a)$ for some polynomial $q \in R[t]$. As $f(a) = 0$, by assumption, we already have $f(t) = q(t)(t-a)$, which is $(t-a) \mid f(t)$.

Conversely for " $\Longleftarrow$ " there is some $q(t) \in R[t]$ such that $f(t) = q(t)(t-a)$ As in (ii) we now use (7.14) in the standard situation $f(a) := \sigma_{\mathbb{1}}(f)$ again, then we find the claim from

$$f(a) \;=\; q(a)\cdot(a-a) \;=\; 0$$

(iv) Obviously induction on the number m of roots, is the way to go: The foundation $m = 1$ already is (iii). So let us proceed with the induction step, that is we assume $f(t) = (t-x_1)\dots(t-x_m)q(t)$ and have another root $f(x_{m+1}) = 0$ such that $x_{m+1} \neq x_i$ for any $i \in 1\dots m$. Then we find

$$0 \;=\; f(x_{m+1}) \;=\; (x_{m+1}-x_1)\dots(x_{m+1}-x_m)\,q(x_{m+1})$$

As all the $(x_{m+1}-x_i) \neq 0$ are non-zero and R is an integral domain, we conclude that $q(x_{m+1}) = 0$. Hence by (iii) there is some polynomial $p \in R[t]$ such that $q(t) = (t-x_{m+1})p(t)$. Replacing q with $(t-x_{m+1})p$ we find the desired representation of f:

$$f(t) \;=\; (t-x_1)\dots(t-x_m)(t-x_{m+1})\,p(t)$$

So let $\{\, x_1,\dots,x_m \,\} = \{\, x \in R \mid f(x) = 0 \,\}$ be the set of roots of f. As the x_i are pairwise distinct, we have just seen, that $f(t) = (t-x_1)\dots(t-x_m)q(t)$ for some $q(t)$. Clearly $q \neq 0$, as else $f = 0$. We now evaluate the degree of f and thereby find the claim

$$\deg(f) \;=\; \deg\big((t-x_1)\dots(t-x_m)\,q(t)\big) \;=\; m+\deg(q) \;\geq\; m$$

(v) Let $d := f-g \in R[t]$, then $\deg(d) \leq \max\{\deg(f),\deg(g)\}$ and for any $x \in R$ we find $f(x) = g(x)$ equivalent to $d(x) = 0$. Combining these arguments we find that, the number of roots of d exceeds the degree of d. Let us summarize:

$$\deg(d) \;\leq\; \max\{\deg(f),\deg(g)\} \;<\; \#\{\, x \in R \mid f(x) = g(x) \,\} \;=\; \#\{\, x \in R \mid d(x) = 0 \,\}$$

But if $d \neq 0$, then (iv) tells us, that the number of roots cannot exceed the degree of d. Due to this contradiction, we conclude $d = 0$ and hence $f = g$.

□

Proof of (7.56):
Property (i) is obvious and (iii) follows from (i) and (ii) immediately: If A is invertible, then $AA^{-1} = E = A^{-1}A$ with $E = \mathbb{1}_n$ again. But then we find $\varphi_{A^{-1}}\varphi_A = \varphi_{AA^{-1}} = \varphi_E = \mathbb{1}_S$ and $\varphi_A\varphi_{A^{-1}} = \varphi_{A^{-1}A} = \varphi_E = \mathbb{1}_S$ such that $\varphi_{A^{-1}} = \big(\varphi_A\big)^{-1}$. The only property that needs some explanation is (ii). And as the t_i generate $S = R[t_1,\dots,t_n]$ is suffices to check $\varphi_B\,\varphi_A(t_i) = \varphi_{AB}(t_i)$ in a short computation. Let $A = (a_{i,j})$ and $B = (b_{j,k})$, then

$$\begin{aligned}\varphi_B\varphi_A(t_i) \;&=\; \varphi_B\left(\sum_{j=1}^n a_{i,j}t_j\right) \;=\; \sum_{j=1}^n a_{i,j}\,\varphi_B(t_j) \;=\; \sum_{j=1}^n a_{i,j}\sum_{k=1}^n b_{j,k}\,t_k \\ &=\; \sum_{k=1}^n\left(\sum_{j=1}^n a_{i,j}b_{j,k}\right)t_k \;=\; \sum_{k=1}^n [AB]_{i,k}\,t_k \;=\; \varphi_{AB}(t_i)\end{aligned}$$

□

Proof of (7.57):

(i) We prove this by induction on n: For $n = 1$ let $m := \deg(f)$ be the degree of f. As $f \neq 0$ is homogeneous this only leaves $f(t_1) = f[m]\, t_1^m$ such that $f(1) = f[m] \neq 0$. For the induction stet we have to distinguish $m := \deg(f)$ and $d := \deg_1(f)$. By (7.40) we can write f in the form

$$f(t_1, \ldots, t_n) \;=\; \sum_{k=0}^{d} f_k(t_1, \ldots, t_{n-1})\, t_n^k$$

where f_k is a homogeneous polynomial of degree $m-k$ and $f_d \neq 0$. By induction hypothesis there are $a_2, \ldots, a_{n-1} \in F$ such that $f_d(1, a_2, \ldots, a_{n-1}) \neq 0$. Then

$$g(x) \;:=\; f(1, a_2, \ldots, a_{n-1}, x) \;=\; \sum_{k=0}^{d} f_k(1, a_2 \ldots, a_{n-1})\, x^k \;\in\; F[x]$$

is a polynomial of degree d over F, in the variable x. But as F is an integral domain, (7.54.(iv)) tells us, that g only has finitely many roots. Yet F is infinite, by assumption, hence there remains some $a_n \in F$, with $g(a_n) \neq 0$. This again is $f(1, a_2, \ldots, a_{n-1}, a_n) \neq 0$ and hence the induction step is completed.

(ii) Let again $m := \deg(f)$ be the degree of f and single out the homogeneous part of f of degree m. That is, we define

$$f_m \;:=\; \sum_{|\alpha|=m} f[\alpha]\, t_1^{\alpha_1} t_2^{\alpha_2} \ldots t_n^{\alpha_n}$$

Then by construction f_m is a homogeneous polynomial of degree m and as $\deg(f) = m$ we have $f_m \neq 0$. Hence by (i) there are $a_2, \ldots, a_n \in F$, such that $f_m(1, a_2, \ldots, a_n) \neq 0$. These elements will do the trick - we only have to provide the why of it. So let us compute

$$g(x_1) \;:=\; f\big(x_1, x_2 + a_2 x_1, \ldots, x_n + a_n x_1\big) \;=\; \sum_{|\alpha| \leq m} f[\alpha]\, x_1^{\alpha_1} \prod_{i=2}^{n} \big(x_i + a_i x_1\big)^{\alpha_i}$$

We now use the binomial rule to evaluate the $(x_i + a_i x_1)^{\alpha_i}$. As *monic* is being decided on the highest term, we are only interested in the leading coefficients

$$\big(x_i + a_i x_1\big)^{\alpha_i} \;=\; \sum_{r=0}^{\alpha_i} \binom{\alpha_i}{r} x_i^{\alpha_i - r} a_i^r x_1^r \;=\; a_i^{\alpha_i} x_1^{\alpha_i} + \text{lower terms in } x_1$$

Inserting this in $g(x_1)$ we find the following equalities for f by straightforward computation

$$\begin{aligned}
g(x_1) \;&=\; \sum_{|\alpha| \leq m} f[\alpha]\, a_2^{\alpha_2} \ldots a_n^{\alpha_n} x_1^{\alpha_1 + \alpha_2 + \cdots + \alpha_n} + \text{lower terms in } x_1 \\
&=\; \sum_{|\alpha| \leq m} f[\alpha]\, (1, a_2, \ldots, a_n)^{\alpha} x_1^{|\alpha|} + \text{lower terms in } x_1 \\
&=\; \left(\sum_{|\alpha| = m} f[\alpha]\, (1, a_2, \ldots, a_n)^{\alpha} \right) x^m + \text{lower terms in } x_1 \\
&=\; f_m(1, a_2, \ldots, a_n)\, x^m + \text{lower terms in } x_1
\end{aligned}$$

But by construction $f_m(1, a_2, \ldots, a_n) \neq 0$ such that we can take $a := f_m(1, a_2, \ldots, a_n)^{-1}$ and thereby have $ag(x_1) = x^m +$ lower terms in x_1. But this is the claim: $ag(x_1) \in R[x_1]$ is monic.

(iii) As $f \neq 0$ the set $A := \{\, \alpha \in \mathbb{N}^n \mid f[\alpha] \neq 0 \,\}$ is finite. In particular $N := \max\{\, \alpha_i \mid \alpha \in A, i \in 1 \ldots n \,\}$ is a finite number. For any $i \in 1 \ldots n$ now define

$$m_i \;:=\; (N+1)^{i-1}$$

That is: for any $\alpha \in (1 \ldots N)^n$ the string $\alpha_n \ldots \alpha_2 \alpha_1$ is the $(N+1)$-adic representation of the number $\langle m \mid \alpha \rangle$. This is to say we get

$$\langle m \mid \alpha \rangle \;=\; \sum_{i=1}^{n} \alpha_i (N+1)^{i-1}$$

In particular $\alpha \mapsto \langle m \mid \alpha_i \rangle$ is injective, as $\langle m \mid \alpha \rangle$ is a number that encodes $\alpha_n \ldots \alpha_2 \alpha_1$. Formally this follows from $\alpha_1 m_1 < \alpha_2 m_2 < \cdots < \alpha_n m_n$ such that we can regain the α_i by *div* and *mod* $N+1$. As $A \subseteq (1 \ldots N)^n$ we have an injective map

$$A \hookrightarrow \mathbb{N} \;:\; \alpha \mapsto \langle m \mid \alpha \rangle$$

And as A is finite there has to be a uniquely determined $\alpha^* \in A$ such that $\langle m \mid \alpha^* \rangle$ is maximal, that is $\langle m \mid \alpha \rangle < \langle m \mid \alpha^* \rangle$ for any $\alpha \in A$ with $\alpha \neq \alpha*$. Now regard

$$g(x_1) \;:=\; f\big(x_1, x_2 + x_1^{m_2}, \ldots, x_n + x_1^{m_n}\big) \;=\; \sum_{\alpha \in A} f[\alpha]\, x_1^{\alpha_1} \prod_{i=2}^{n} \big(x_i + x_1^{m_i}\big)^{\alpha_i}$$

Again we evaluate any $(x_i + x_1^{m_i})^{\alpha_i}$ using the binomial rule. As *monic* is being decided on the highest term, we are only interested in the leading coefficients again

$$\big(x_i + x_1^{m_1}\big)^{\alpha_i} \;=\; \sum_{r=0}^{\alpha_i} \binom{\alpha_i}{r} x_i^{\alpha_i - r} x_1^{m_i r} \;=\; x_1^{m_i \alpha_i} + \text{lower terms in } x_1$$

Inserting this in $g(x_1)$ we find the following equalities for f. Also note that $m_1 = 1$ such that $\alpha_1 + m_2\alpha_2 + \cdots + m_n\alpha_n = \langle m \mid \alpha \rangle$ which enables us to compute

$$\begin{aligned} g(x_1) \;&=\; \sum_{\alpha \in A} f[\alpha]\, x_1^{\alpha_1 + m_2\alpha_2 + \cdots + m_n\alpha_n} + \text{lower terms in } x_1 \\ &=\; \sum_{\alpha \in A} f[\alpha]\, x_1^{\langle m \mid \alpha \rangle} + \text{lower terms in } x_1 \\ &=\; f[\alpha^*]\, x_1^{\langle m \mid \alpha^* \rangle} + \text{lower terms in } x_1 \end{aligned}$$

As $\alpha^* \in A$ we have $f[\alpha^*] \neq 0$ and therefore we can take $a := f[\alpha^*]^{-1}$ and thereby have $ag(x_1) = x^{\langle m \mid \alpha^* \rangle} +$ lower terms in x_1. But this is the claim: $ag(x_1) \in R[x_1]$ is monic.

□

Proof of (7.58):

(i) Let us first prove that in case of an integral domain R the determinant of the Vandermonde matrix

truly has the form given in the claim: To do this let us first consider the case that there are some $i < j \in 1 \dots n$ such that $x_i = x_j$ are equal. In this case two separate rows of the Vandermonde matrix are equal and hence the determinant is zero. On the other hand the product vanishes as well, as $x_j - x_i = 0$ and hence

$$\det\left(\mathrm{Van}(x_1, \dots, x_n)\right) \;=\; 0 \;=\; \prod_{1 \leq i < j \leq n} (x_j - x_i)$$

Thus let us assume that for any $i \neq j \in 1 \dots n$ the elements $x_i \neq x_j$ are distinct. We now use induction on the number n - the case $n = 1$ is true, as in this case $\mathrm{Van}(x_1) = (1)$ such that we have $\det(\mathrm{Van}(x_1)) = 1$. But also the set $\left\{ (i,j) \in (1 \dots n)^2 \mid i < j \right\} = \emptyset$ is empty and the product over the empty set has been defined to be 1. However, to eliminate all doubt, we also found the induction on $n = 2$, in this case

$$\det \begin{pmatrix} 1 & x_1 \\ 1 & x_2 \end{pmatrix} \;=\; (x_2 - x_1) \;=\; \prod_{1 \leq i < j \leq 2} (x_j - x_i)$$

is plain to see. In the induction step for $n \geq 2$ we pick up a variable z and regard the polynomial ring $R \subseteq R' := R[z]$ instead. Then we append the n-tuple $x := (x_1, \dots, x_n) \in R^n$ to $x' := (x_1, \dots, x_n, z) \in (R')^{n+1}$ and define the polynomial $h \in R' = R[z]$ to be the following

$$h(z) \;:=\; \det\left(\mathrm{van}(x')\right) \;=\; \det \begin{pmatrix} 1 & x_1 & \cdots & x_1^n \\ \vdots & \vdots & & \vdots \\ 1 & x_n & \cdots & x_n^n \\ 1 & z & \cdots & z^n \end{pmatrix}$$

We now use the formula of Laplace (4.55.(v)) to evaluate this determinant by expanding along the lowest row. For sake of easy readability let us use the common abbreviation $|A| := \det(A)$ of a determinant. Then expansion yields the following formula

$$h(y) \;=\; (-1)^n \begin{vmatrix} x_1 & \cdots & x_1^n \\ \vdots & & \vdots \\ x_n & \cdots & x_n^n \end{vmatrix} + \cdots + \begin{vmatrix} 1 & \cdots & x_1^{n-1} \\ \vdots & & \vdots \\ 1 & \cdots & x_n^{n-1} \end{vmatrix} z^n$$

From this we see that h is a polynomial of degree n in z. We also see, that the leading coefficient of h is the determinant of the Vandermonde matrix of x. By induction hypothesis, this is

$$\Delta \;:=\; \mathrm{lc}(h) \;=\; \det\left(\mathrm{Van}(x)\right) \;=\; \prod_{1 \leq i < j \leq n} (x_j - x_i)$$

But from the definition of h it is clear, that $h(x_i) = 0$, as for $z = x_i$ the last row is just a copy of the i-th row and hence the determinant vanishes. Recall that we assumed the x_i to be pairwise distinct, that is we have found n distinct roots of the polynomial h of degree n. As R is an integral domain (7.54.(iv)) tells us, that h splits into linear factors

$$h(z) \;=\; \Delta\,(z - x_1) \dots (z - x_n)$$

Now $h(z)$ finally is the determinant of the Vandermonde matrix of x' once we insert $z = x_{n+1}$. Doing this we finally find the claim for $n+1$, as we then compute

$$\begin{aligned} h(x_{n+1}) &= \det(\mathrm{van}(x_1,\ldots,x_n,x_{n+1})) \\ &= \left(\prod_{1\le i<j\le n}(x_j - x_i)\right)(x_{n+1}-x_1)\ldots(x_{n+1}-x_n) \\ &= \prod_{1\le i<j\le n+1}(x_j - x_i) \end{aligned}$$

(ii) By construction we have $\deg(L_j) = n-1$, as any $t - x_i$ is a monic polynomial of degree 1. Hence we have $L_j \in \mathcal{P}_n$. Let us first prove that the L_j form a linearly independent subset of $\mathcal{P}_n$. That is we assume that

$$a_1 L_1(t) + \cdots + a_n L_n(t) \;=\; \mathbf{0} \;\in\; R[t]$$

for some $a_j \in R$. As we have $L_j(x_i) = \delta_{i,j}$ we may insert x_i into this equation and thereby find $0 = \mathbf{0}(x_i) = \sum_j a_j L_j(x_i) = a_i$. As this is true for any $i \in 1\ldots n$ this is the linear independence. Now let $f := \sum_j y_j L_j \in \mathcal{P}_n$ then by the same reasoning we get

$$f(x_i) \;=\; \sum_{j=1}^{n} y_j\, L_j(x_i) \;=\; \sum_{j=1}^{n} y_j\, \delta_{i,j} \;=\; y_i$$

Given any other polynomial $g \in \mathcal{P}_n$ let $y_i := g(x_i)$ and build up f as before $f := \sum_j y_j L_j$. Then we have $g(x_i) = y_i = f(x_i)$, that is f and g agree at n locations $x_1,\ldots,x_n$. As both are of degree $\deg(g)$, $\deg(f) < n$ we find from (7.54.(v)) that $f = g$. Hence the set $\{L_1,\ldots,L_n\}$ also is a generating set, of $\mathcal{P}_n$ and hence a basis.

(iii) If we insert x_i into the ansatz $f = a_0N_0 + a_1N_1 + \cdots + a_{n-1}N_{n-1}$ this equation turns into $y_i = a_0N_0(x_i) + a_1N_1(x_i) + \cdots + a_{n-1}N_{n-1}(x_i)$. If we combine these n equations into a single matrix equation, this reads as

$$\begin{pmatrix} N_0(x_1) & N_1(x_1) & N_2(x_1) & \cdots & N_{n-1}(x_1) \\ N_0(x_2) & N_1(x_2) & N_2(x_2) & \cdots & N_{n-1}(x_2) \\ \vdots & \vdots & \vdots & & \vdots \\ N_0(x_n) & N_1(x_n) & N_2(x_n) & \cdots & N_{n-1}(x_n) \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$$

However $N_0(t) = \mathbf{1}$ such that $N_0(x_i) = 1$ for any $i \in 1\ldots n$. And it also is clear that $N_j(x_i) = 0$ whenever $i \le j$, by construction of the $N_j(t)$. Hence this matrix is truly reduced to a lower triangular matrix, as given in the claim of the Newtonian interpolation method. The determinant of this lower triangular matrix truly is

$$\prod_{j=1}^{n} N_{j-1}(x_j) \;=\; \prod_{j=1}^{n}\prod_{i=1}^{j-1}(x_j - x_i) \;=\; \prod_{1\le i<j\le n}(x_j - x_i)$$

□

Proof of (7.59):

(i) As F is a field, it also is an integral domain. And as the x_i are pairwise distinct, the determinant of the Vandermonde matrix $\mathrm{Van}(x_1,\ldots,x_n)$ is non-zero, as any factor $x_j - x_i \neq 0$ is non-zero

$$\det\Big(\mathrm{Van}(x_1,\ldots,x_n)\Big) \;=\; \prod_{1\leq i<j\leq n}(x_j - x_i) \;\neq\; 0$$

In a field F this means, that the determinant is invertible and hence the Vandermonde-matrix is invertible, by (4.63.(ii)). Then we find a polynomial f satisfying (1) and (2) by (7.58.(i)). Its coefficients are given to be

$$\begin{pmatrix} f[0] \\ f[1] \\ \vdots \\ f[n-1] \end{pmatrix} = \begin{pmatrix} 1 & x_1 & \cdots & x_1^{n-1} \\ 1 & x_2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & x_n & \cdots & x_n^{n-1} \end{pmatrix}^{-1} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$$

(ii) If F is finite, say $F = \{ x_0,\ldots,x_n \}$, and $u : F \to F$ is any function, then let $y_i := u(x_i)$. By (i) there is a polynomial $f \in F[t]$ of degree $\deg(f) \leq n$ satisfying $f(x_i) = y_i$ for any $i \in 0\ldots n$. In particular $P_f = u$ and hence P is surjective. Yet $\#\mathbb{F}(F,F) = (n+1)^{n+1}$ is a finite set, whereas $F[t] = \mathbb{F}(\mathbb{N},F)$ is infinite. In particular $P : F[t] \to \mathcal{F}(F,F)$ cannot be injective.

If F is infinite then we consider two polynomials $f, g \in F[t]$ such that $P_f = P_g$. That is $f(x) = g(x)$ for any $x \in F$ and hence $\{ x \in F \mid f(x) = g(x) \} = F$ is infinite. In particular this set has more elements than the degrees of f and g, such that we get $f = g$ from (7.54.(v)). That is P is injective. Now define the function $u : F \to F$ by $u(0) := 1$ and $u(x) := 0$ for any $x \in F^*$. Suppose there was a polynomial $f \in F[t]$ such that $P_f = u$, then f has infinitely many roots $\mathbb{V}(f) = F^*$. In particular $f = 0$ by (7.54.(iv)). But then $f(0) = 0 \neq 1 = u(0)$, a contradiction. Hence there is no $f \in F[t]$ with $P_f = u$, such that P is not surjective.

□

Proof of (7.61):

(ii) As $0(x) = 0$ for any $x \in R^I$ we clearly have $0 \in \mathbb{I}(X)$. Now consider $f, g \in \mathbb{I}(X)$. That is for any $x \in X$ we have $f(x) = 0 = g(x)$. In particular $(f+g)(x) = f(x) + g(x) = 0 + 0 = 0$ and $(-f)(x) = -f(x) = -0 = 0$ such that $f+g$, $-f \in \mathbb{I}(X)$ again. And for any $h \in R[t_i \mid i \in I]$ we get $(fh)(x) = f(x)h(x) = 0 \cdot h(x) = 0$ such that also $fh \in \mathbb{I}(X)$. Altogether $\mathbb{I}(X)$ is an ideal.

Now assume that $\mathrm{NIL}(R) = 0$ and consider some $f \in \sqrt{\mathbb{I}(X)}$. That is $f^k \in \mathbb{I}(X)$ for some $k \in \mathbb{N}$. Then for any $x \in X$ we get $0 = f^k(x) = f(x)^k$. That is $f(x) \in R$ is nilpotent and hence $f(x) = 0$ by $\mathrm{NIL}(R) = 0$. As $x \in X$ has been arbitrary this is $f \in \mathbb{I}(X)$ and the converse inclusion is true in general. Thus $\mathbb{I}(X)$ then is a radical ideal.

(iii) As $F \subseteq \mathfrak{a}$ we clearly have $\mathbb{V}(\mathfrak{a}) \subseteq \mathbb{V}(F)$. Conversely consider any $x \in \mathbb{V}(F)$. If now $f \in \mathfrak{a}$, then f is of the form $f = g_1 f_1 + \cdots + g_n f_n$ for some $f_\lambda \in F$. And hence, as any $f_\lambda(x) = 0$ we get $f(x) = g_1(x)\,0 + \cdots + g_n(x)\,0 = 0$, which implies $x \in \mathbb{V}(\mathfrak{a})$.

Now assume that $\mathrm{NIL}(R) = 0$, as $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$ we again get $\mathbb{V}(\sqrt{\mathfrak{a}}) \subseteq \mathbb{V}(\mathfrak{a})$. Conversely consider any $x \in \mathbb{V}(\mathfrak{a})$. If now $f \in \sqrt{\mathfrak{a}}$, then there is some $k \in \mathbb{N}$ such that $f^k \in \mathfrak{a}$ and hence $f(x)^k = f^k(x) = 0$. But as $\mathrm{NIL}(R) = 0$, this implies $f(x) = 0$ and hence $x \in \mathbb{V}(\sqrt{\mathfrak{a}})$.

(iv) For any $X \subseteq Y \subseteq R^I$ it is clear that $\mathbb{I}(Y) \subseteq \mathbb{I}(X)$, as then $f(x) = 0$ for any $x \in Y$ implies $f(x) = 0$ for any $x \in X$, too. And likewise $\mathfrak{a} \subseteq \mathfrak{b}$ implies $\mathbb{V}(\mathfrak{b}) \subseteq \mathbb{V}(\mathfrak{a})$, as then $f(x) = 0$ for any $f \in \mathfrak{b}$ implies $f(x) = 0$ for any $f \in \mathfrak{a}$, too.

By (0.22) property (b) it suffices to check $X \subseteq \mathbb{VI}(X)$ and $F \subseteq \mathbb{IV}(F)$ for any $X \subseteq R^I$ and $F \subseteq R[t_i \mid i \in I]$ respectively. But if $x \in X$ and $f \in \mathbb{I}(X)$ then it is clear that $f(x) = 0$ such that $x \in \mathbb{V}(f)$ again. But as this is true for any $x \in X$ and any $f \in \mathbb{I}(X)$ this already is $X \subseteq \mathbb{VI}(X)$. Likewise if $f \in F$ and $x \in \mathbb{V}(F)$, then $f(x) = 0$ such that $f \in \mathbb{I}(x)$ again.

(i) $f \in \mathbb{I}(X)$ is $\{f\} \subseteq \mathbb{I}(X)$ which implies $\mathbb{VI}(X) \subseteq \mathbb{V}(f)$. But as we have seen $X \subseteq \mathbb{VI}(X)$ in (iv) this implies $X \subseteq \mathbb{V}(f)$. Again this means $f(x) = 0$ for any $x \in X$ and hence $f \in \mathbb{I}(X)$.

$x \in \mathbb{V}(F)$ is $\{x\} \subseteq \mathbb{V}(F)$ which implies $\mathbb{IV}(F) \subseteq \mathbb{I}(x)$. But as we have seen $F \subseteq \mathbb{IV}(F)$ in (iv) this implies $F \subseteq \mathbb{I}(x)$. Again this means $f(x) = 0$ for any $f \in F$ and hence $x \in \mathbb{V}(F)$.

(v) Clearly $\mathbb{V}(0) = R^I$, as for any $x \in R^I$ we have $0(x) = 0$. Similarly $\mathbb{V}(R[t_i \mid i \in I]) = \emptyset$, as for any $x \in R^I$ we have $\mathbf{1}(x) = 1$ and $1 \neq 0$, as R is an integral domain. The next claim is

$$\mathbb{V}(\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n) \quad \subseteq \quad \mathbb{V}(\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n) \quad \subseteq \quad \mathbb{V}(\mathfrak{a}_1) \cup \cdots \cup \mathbb{V}(\mathfrak{a}_n)$$

As for any $\lambda \in 1 \ldots n$ we have the inclusions $\mathfrak{a}_1 \ldots \mathfrak{a}_n \subseteq \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n \subseteq \mathfrak{a}_\lambda$ the algebraic sets satisfy the converse inclusions $\mathbb{V}(\mathfrak{a}_\lambda) \subseteq \mathbb{V}(\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n) \subseteq \mathbb{V}(\mathfrak{a}_1 \ldots \mathfrak{a}_n)$. And as this is true for any $\lambda \in 1 \ldots n$ we get $\mathbb{V}(\mathfrak{a}_1) \cup \cdots \cup \mathbb{V}(\mathfrak{a}_n) \subseteq \mathbb{V}(\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n)$. Now suppose R is an integral domain, then we even get $\mathbb{V}(\mathfrak{a}_1 \ldots \mathfrak{a}_n) = \mathbb{V}(\mathfrak{a}_1) \cup \cdots \cup \mathbb{V}(\mathfrak{a}_n)$, because of: Suppose there was some $x \in \mathbb{V}(\mathfrak{a}_1 \ldots \mathfrak{a}_n)$ such that for any $\lambda \in 1 \ldots n$ we had $x \notin \mathbb{V}(\mathfrak{a}_\lambda)$. That is there is some $f_\lambda \in \mathfrak{a}_\lambda$ such that $f_\lambda(x) \neq 0$. But as R is an integral domain, this implies $(f_1 \ldots f_n)(x) = f_1(x) \ldots f_n(x) \neq 0$. Yet $f_1 \ldots f_n \in \mathfrak{a}_1 \ldots \mathfrak{a}_n$ such that we also have $(f_1 \ldots f_n)(x) = 0$. This contradiction is solved by concluding $x \in \mathbb{V}(\mathfrak{a}_\lambda)$ for some $\lambda \in 1 \ldots n$. So we will next prove

$$\mathbb{V}\left(\sum_{\lambda \in \Lambda} \mathfrak{a}_\lambda\right) \quad = \quad \bigcap_{\lambda \in \Lambda} \mathbb{V}(\mathfrak{a}_\lambda)$$

where R need not be an integral domain, any longer. The inclusion "$\subseteq$" is clear, as for any $\mu \in \Lambda$ we have $\mathfrak{a}_\mu \subseteq \sum_\lambda \mathfrak{a}_\lambda$ and hence the converse inclusion for the algebraic sets. For the converse inclusion consider any $x \in \bigcap_\lambda \mathbb{V}(\mathfrak{a}_\lambda)$ and any $f \in \sum_\lambda \mathfrak{a}_\lambda$. That is f is of the form $f = f_1 + \cdots + f_k$ for some $f_j \in \mathfrak{a}_{\lambda(j)}$. Then clearly $f(x) = f_1(x) + \cdots + f_k(x) = 0$, such that we also get $x \in \mathbb{V}(\sum_\lambda \mathfrak{a}_\lambda)$.

Thus we have proved all the claims for algebraic sets and we turn our attention to the vanishing ideals: As with algebraic sets $\emptyset \subseteq R^I$ poses no restriction on polynomials and hence we have $\mathbb{I}(\emptyset) = R[t_i \mid i \in I]$. And as $X_\lambda \subseteq \bigcup_\lambda X_\lambda$ - we have $\mathbb{I}(\bigcup_\lambda X_\lambda) \subseteq \mathbb{I}(X_\lambda)$ for any $\lambda \in \Lambda$ such that $\mathbb{I}(\bigcup_\lambda X_\lambda) \subseteq \bigcap_\lambda \mathbb{I}(X_\lambda)$. And if conversely $f \in \bigcap_\lambda \mathbb{I}(X_\lambda)$ then for any $x \in \bigcup_\lambda X_\lambda$ there is some $\mu \in \Lambda$ with $x \in X_\mu$ and hence $f \in \mathbb{I}(X_\mu)$ such that $f(x) = 0$. Finally regard any $f \in \sum_\lambda \mathbb{I}(X_\lambda)$, that is f is of the form $f = f_1 + \cdots + f_k$ for some $f_j \in \mathbb{I}(X_{\lambda(j)})$. If now $x \in \bigcap_\lambda X_\lambda$ then $f(x) = f_1(x) + \cdots + f_k(x) = 0$ and hence $f \in \mathbb{I}(\bigcap_\lambda X_\lambda)$.

(vi) If $R \neq 0$, then $1 \neq 0$ And hence we get $\mathbf{1}(x) = 1 \neq 0$ for any $x \in R^I$. And as $\mathbf{1} \in R[t_i \mid i \in I]$ this implies $\mathbb{V}(R[t_i \mid i \in I]) = \emptyset$. If R is an integral domain, then $R \neq 0$ is part of the definition.

Now suppose R is an infinite integral domain, then we wish to prove $\mathbb{I}(R^I) = 0$. That is we consider any $f \in \mathbb{I}(R^I)$, which is $\mathbb{V}(f) = R^I$, and have to show $f = 0$. As $f \in R[t_i \mid i \in I]$ in truth it is contained in some finite polynomial ring, that is $f \in R[t_i \mid i \in \omega]$ for some finite subset $\omega \subseteq I$, according to (7.23.(i)). For ease of notation let $\omega = \{1, \ldots, n\}$ and use induction on n: For $n = 1$ we have $f \in R[t_1]$ a polynomial in one variable over R. But for $f \in R[t_1]$ with $f \neq 0$ we know $\#\mathbb{V}(f) \leq \deg(f)$, which is finite, due to (7.54.(vi)). But as R is infinite and $\mathbb{V}(f) = R$ the set $\mathbb{V}(f)$ is infinite and this can only mean $f = 0$. Now for the induction step $n \geq 2$: Then we define $f_1(t_1) := f(t_1, 0, \ldots, 0) \in R[t_1]$. This yields $f_1(x_1) = f(x_1, 0, \ldots, 0) = 0$ for any $x_1 \in R$ and hence $f_1 = 0$ by the case $n = 1$. Thus f actually only depends on the variables $f(t_2, \ldots, t_n)$, so by induction hypothesis we get $f = 0$ again.

□

Proof of (7.62):

(i) As $\mathbb{VI}(X)$ is a closed set by construction and $X \subseteq \mathbb{VI}(X)$, it is clear, that $\overline{X} \subseteq \mathbb{VI}(X)$. Conversely, if $C \subseteq R^I$ is a closed set, then C is of the form $C = \mathbb{V}(\mathfrak{a})$ for some $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R[t_i \mid i \in I]$. Now, if $X \subseteq C$, then this implies $\mathbb{I}(C) \subseteq \mathbb{I}(X)$ from which we get $\mathbb{VI}(X) \subseteq \mathbb{VI}(C)$. Due to the Galois connection (7.61.(iv)) we have $\mathbb{VI}(C) = \mathbb{VIV}(\mathfrak{a}) = \mathbb{V}(\mathfrak{a}) = C$ and thereby $\mathbb{VI}(X) \subseteq C$. Thus $\mathbb{VI}(X)$ is contained in any closed set above X and this implies $\mathbb{VI}(X) \subseteq \overline{X}$, too.

(ii) If $\mathfrak{a} = 0$ then $\mathbb{V}(\mathfrak{a}) = R^I$ is clear. Conversely, if $\mathbb{V}(\mathfrak{a}) = R^I$ then $\mathfrak{a} \subseteq \mathbb{IV}(\mathfrak{a}) = \mathbb{I}(R^I) = 0$, according to (7.61.(iv)) and (7.61.(vi)). But $\mathfrak{a} \subseteq 0$ means $\mathfrak{a} = 0$.

□

Proof of (7.66):
The proof of all these statements relies in short, uninstructive computations. Thereby every statement is an easy consequence of the previous one and the reader looses nothing if he skips the proof entirely.

(i) By definition $s_k^{(n)}$ is a sum of terms $t_{\alpha(1)} \ldots t_{\alpha(k)}$ where $\alpha \in \mathrm{Asc}(k, n)$. Any of these terms is of degree k and hence $s_k^{(n)}$ is of degree k, as well.

(i) Let us abbreviate $s_k := s_k^{(n)}$ and $s := (s_1, \ldots, s_n) \in R[t_1, \ldots, t_n]^n$. Then in (i) we have seen $\deg(s_k) = k$ and hence for a monomial $f = t^\alpha$ where $\alpha \in \mathbb{N}^n$ the claim is straightforward to see

$$\deg\big(t^\alpha(s)\big) \;=\; \deg\big(s^\alpha\big) \;=\; \sum_{k=1}^{n} \deg\big(s_k^{\alpha_i}\big) \;=\; \sum_{k=1}^{n} \alpha_k \cdot k \;=\; \mathrm{wgt}\big(t^\alpha\big)$$

Thus for an arbitrary polynomial $f \in R[t_1, \ldots, t_n]$ this computation is inherited, as both, the degree and the weight, are defined to be the maximum among all $\alpha \in \mathbb{N}^n$ with $f[\alpha]$. Formally

$$\begin{aligned} \deg(f(s)) &= \max\{\, \deg(s^\alpha) \mid \alpha \in \mathbb{N} \text{ and } f[\alpha] \neq 0 \,\} \\ &= \max\{\, \mathrm{wgt}(t^\alpha) \mid \alpha \in \mathbb{N} \text{ and } f[\alpha] \neq 0 \,\} \;=\; \mathrm{wgt}(f) \end{aligned}$$

(ii) If $k = 1$ then $s_1^{(n)} = t_1 + \cdots + t_n = (t_1 + \cdots + t_{n-1}) + 1 \cdot t_n$ which is $s_1^{(n-1)} + s_0^{(n-1)} \cdot t_n$ again. Hence we may continue with $k \geq 2$. Clearly, for $n \geq 2$, we can decompose $\mathrm{Asc}(k, n)$ into two separate parts: We either have $\alpha(k) = n$ or not. If not, then $\alpha \in \mathrm{Asc}(k, n-1)$ and if $\alpha(k) = n$,

then β is of the form $\alpha = (\alpha', n)$ where $\alpha' = (\alpha(1), \ldots, \alpha(n-1)) \in \mathrm{Asc}(k-1, n-1)$. Thus we have established a disjoint union

$$\mathrm{Asc}(k,n) \;=\; \mathrm{Asc}(k,n-1) \cup \left\{ (\alpha', n) \mid \alpha' \in \mathrm{Asc}(k-1,n-1) \right\}$$

Thus the sum over $\alpha \in \mathrm{Asc}(k,n)$ that has been used in the definition of $s_k^{(n)}$ can be split into two parts: A sum over $\alpha \in \mathrm{Asc}(k,n-1)$ and a sum over $\alpha' \in \mathrm{Asc}(k-1,n-1)$, where we have to rebuild α as (α', n) and hence $t_{\alpha(1)} \ldots t_{\alpha(k-1)} t_n$

$$\begin{aligned} s_k^{(n)} &= \sum_{\alpha \in \mathrm{Asc}(k,n)} t_{\alpha(1)} \ldots t_{\alpha(k)} \\ &= \sum_{\alpha \in \mathrm{Asc}(k,n-1)} t_{\alpha(1)} \ldots t_{\alpha(k)} + \sum_{\alpha' \in \mathrm{Asc}(k-1,n-1)} t_{\alpha(1)} \ldots t_{\alpha(k-1)} t_n \\ &= s_k^{(n-1)} + s_{k-1}^{(n-1)} \cdot t_n \end{aligned}$$

(iii) The proof will be by induction on n, in case $n = 1$ we only have $k = 0$ and hence only need $(-1)^{n-k} s_{n-k}^{(n)} = (-1)^1 s_1^{(1)} = -t_1$. For this we get $-t_1(a_1) = -a_1$ and hence we are done. For the induction step $n \geq 2$ we will use the abbreviation $a' := (a_1, \ldots, a_{n-1})$. With this we use the induction hypothesis right away

$$\begin{aligned} & (t-a_1) \ldots (t-a_{n-1}) \, (t-a_n) \\ = \;& \left(\sum_{k=0}^{n-1} (-1)^{n-1-k} \, s_{n-1-k}^{(n-1)}(a') \, t^k \right) (t-a_n) \\ = \;& \sum_{k=0}^{n-1} (-1)^{n-1-k} \, s_{n-1-k}^{(n-1)}(a') \, t^{k+1} - \sum_{k=0}^{n-1} (-1)^{n-1-k} \, s_{n-1-k}^{(n-1)}(a') a_n \, t^k \\ = \;& \sum_{k=1}^{n} (-1)^{n-k} \, s_{n-k}^{(n-1)}(a') \, t^k + \sum_{k=0}^{n-1} (-1)^{n-k} \, s_{n-1-k}^{(n-1)}(a') a_n \, t^k \\ = \;& t^n + \sum_{k=1}^{n-1} (-1)^{n-k} \left(s_{n-k}^{(n-1)}(a') + s_{n-1-k}^{(n-1)}(\widehat{a}) a_n \right) t^k + (-1)^n s_{n-1}^{(n-1)}(a') a_n \end{aligned}$$

But $s_{n-1}^{(n-1)}(a') a_n = a_1 \ldots a_{n-1} a_n = a_1 \ldots a_n = s_n^{(n)}(a)$ is clear and by the recursion formula of (ii) we also find $s_{n-k}^{(n-1)}(a') + s_{n-1-k}^{(n-1)}(a') a_n = s_k^{(n)}(a)$. Thus we have obtained our claim

$$(t-a_1) \ldots (t-a_{n-1}) \, (t-a_n) \;=\; t^n + \sum_{k=1}^{n-1} (-1)^{n-k} \, s_k^{(n)}(a) \, t^k + (-1)^n s_n^{(n)}(a)$$

□

Proof of (7.67):

(ii) We need to show that all the coefficient polynomials $f[k] \in R[t_1, \ldots, t_{n-1}]$ are symmetric. Thus suppose we are given any permutation $\sigma \in S_{n-1}$. Then we can extend σ to S_n by letting $\sigma(n) := n$. As f is symmetric, we have $\sigma f = f$ by assumption. And as $f \mapsto \sigma f$ is a homomorphism also

$$f \;=\; \sigma f \;=\; \sigma f[0] + \sigma f[1] \, t_n + \cdots + \sigma f[d] \, t_n^d$$

Let $S := R[t_1,\dots,t_{n-1}]$, then $\{\, t_n^k \mid k \in \mathbb{N} \,\}$ is an S-basis of $S[t_n]$. Thus the above linear combination is a basis representation of f. Comparing coefficients with $f = f[0] + f[1]t_n + \cdots + f[d]t^d$ we find $f[k] = \sigma f[k]$. And as this is true for any $\sigma \in S_{n-1}$ this means that $f[k]$ is symmetric.

(iii) We will first check that $g(s_1,\dots,s_n) = 0$ implies $g = 0$, for any polynomial $g \in R[t_1,\dots,t_n]$. To do this write g in the form $g = g[0] + g[1]\,t_n + \cdots + g[d]\,t_n^d$, as in (ii). Now suppose the implication was false, i.e. there is some n and some $0 \neq g \in R[t_1,\dots,t_n]$ such that $g(s_1,\dots,s_n) = 0$. Then we choose n to be the minimal number of variables for which such a counterexample g exists. And we choose g in such a way that the t_n-degree d of g is minimal, too. In particular $g[0] \neq 0$, as we else could scratch one t_n, as this is a monic polynomial. In the case $n = 1$ we have $s_1 = t_1$ such that $0 = g(s_1) = g(t_1)$ is $g = 0$. Thus the counterexample must feature $n \geq 2$.

Let $r_k(t_1,\dots,t_{n-1}) := s_k(t_1,\dots,t_{n-1},0) \in R[t_1,\dots,t_{n-1}]$, then $r_n = 0$ and $r_k = s_k^{(n-1)}$ is the k-th elementary symmetric polynomial in $n-1$ variables, for $1 \leq k < n$, according to (7.66.(ii)). And as $g(s_1,\dots,s_n) = 0 \in R[t_1,\dots,t_n]$ we find in particular

$$g(r_1,\dots,r_{n-1},0) \;=\; g(s_1,\dots,s_n)(t_1,\dots,t_{n-1},0) \;=\; 0 \;\in\; R[t_1,\dots,t_{n-1}]$$

Now recall that we have written g as an element of $R[t_1,\dots,t_{n-1}][t_n]$, then we find $g(s_1,\dots,s_n) = g[0](s_1,\dots,s_{n-1}) + \cdots + g[d](s_1,\dots,s_{n-1})\,s_n^d$. And if we insert $(t_1,\dots,t_{n-1},0)$ into this expression, we end up with

$$0 \;=\; g(r_1,\dots,r_{n-1},0) \;=\; g(s_1,\dots,s_n)(t_1,\dots,t_{n-1},0) \;=\; g[0](r_1,\dots,r_{n-1})$$

Recall that n was taken to be minimal with this property, but here we have found a polynomial $0 \neq g[0] \in R[t_1,\dots,t_{n-1}]$ such that $g[0](r_1,\dots,r_{n-1}) = 0$. This contradicts the minimality of n. And hence there is no counterexample - the implication is universally true.

$$g(s_1,\dots,s_n) \;=\; 0 \quad\Longrightarrow\quad g \;=\; 0$$

If now f, $g \in R[t_1,\dots,t_n]$ with $f(s_1,\dots,s_n) = g(s_1,\dots,s_n)$ then $(f-g)(s_1,\dots,s_n) = 0$ and by the above implication this yields $f - g = 0$ and hence $f = g$. The converse direction is trivial.

(i) As $\sigma 0 = 0$ and $\sigma 1 = 1$ we see that 0 and 1 are symmetric polynomials. And if $a \in R$ and f, $g \in R[t_1,\dots,t_n]$ are symmetric polynomials, then by (7.65) we also have $\sigma(af) = a\sigma f = af$ and likewise $\sigma(f+g) = \sigma f + \sigma g = f + g$ and $\sigma(f \cdot g) = \sigma f \cdot \sigma g = f \cdot g$, such that af, $f+g$ and $f \cdot g$ are symmetric, again. That is the symmetric polynomials form a subalgebra of $R[t_1,\dots,t_n]$.

Thus we only need to verify, that this algebra is truly generated by the elementary symmetric polynomials. To do this we will prove the following statement: For any symmetric polynomial $s \in R[t_1,\dots,t_n]$ there is a polynomial $g \in R[t_1,\dots,t_n]$ such that we get

$$\mathrm{wgt}(g) \;\leq\; \deg(s) \quad\text{and}\quad s \;=\; g\left(s_1^{(n)},\dots,s_n^{(n)}\right)$$

We start by induction on the number n of variables. In the case $n = 1$ we have $s_1 = t_1$ and hence we may choose $g := s$. Thus we may turn to $n \geq 2$. Then we write s (and any other polynomial of

$R[t_1,\dots,t_n]$) as an element of $R[t_1,\dots,t_{n-1}][t_n]$ once more, that is

$$s(t_1,\dots,t_n) \;=\; s[0] + s[1]\,t_n + \cdots + s[d]\,t_n^d$$

By (ii) we know that $s[0]$ is symmetric, too and hence by induction hypothesis there is a polynomial $q \in R[t_1,\dots,t_{n-1}]$ such that we get $\mathrm{wgt}(q) \le \deg(s[0]) \le \deg(s)$ and $s[0] = q(r_1,\dots,r_{n-1})$ where we abbreviated $s_k := s_k^{(n)}$ and $r_k := s_k^{(n-1)} = s_k[0]$ again.

We now start a second induction on the degree $\deg(s)$ of s. In the case $\deg(s) \le 0$ we see that s is constant and hence we may choose $g := s$. Thus we may regard $\deg(s) \ge 1$. As the symmetric polynomials form an algebra we find that

$$\widetilde{s} \;:=\; s - q(s_1,\dots,s_{n-1}) \;\in\; R[t_1,\dots,t_n]$$

is symmetric, too. By construction we have $\widetilde{s}[0] = s[0] - q(r_1,\dots,r_{n-1}) = 0$ such that t_n divides $\widetilde{s}$. And it is clear that we find an upper bound of the degree of $\widetilde{s}$ by

$$\begin{aligned}\deg(\widetilde{s}) \;&\le\; \max\{\,\deg(s),\,\deg(q(r_1,\dots,r_{n-1})\,\}\\ &\le\; \max\{\,\deg(s),\,\mathrm{wgt}(q)\,\} \;=\; \deg(s)\end{aligned}$$

But as $\widetilde{s}$ is symmetric and $t_n \mid \widetilde{s}$ we see that for any $k \in 1\dots n$ we get $t_k \mid \widetilde{s}$ and hence $s_n = t_1 \dots t_n \mid \widetilde{s}$. Let us now denote $\widetilde{s} = s_n \cdot \widehat{s}$, then we claim that $\widehat{s}$ is symmetric, too: For any $\sigma \in S_n$ we have $s_n\widehat{s} = \widetilde{s} = \sigma\widetilde{s} = (\sigma s_n)\cdot(\sigma\widehat{s}) = s_n \cdot (\sigma\widehat{s})$. As s_n is monic, this implies $\widehat{s} = \sigma\widehat{s}$ and as this is true for any $\sigma \in S_n$ we see that $\widehat{s}$ is symmetric. Now

$$\deg(\widehat{s}) \;=\; \deg(\widetilde{s}) - \deg(s_n) \;\le\; \deg(s) - n \;<\; \deg(s)$$

Thus by induction hypothesis (on $\deg(s)$) there is a symmetric polynomial $p \in R[t_1,\dots,t_n]$ such that $\mathrm{wgt}(p) \le \deg(\widehat{s}) \le \deg(s) - n$ and $\widehat{s} = p(s_1,\dots,s_n)$. Altogether we got

$$\begin{aligned} s \;&=\; \widetilde{s} + q(s_1,\dots,s_{n-1})\\ &=\; s_n\widehat{s} + q(s_1,\dots,s_{n-1})\\ &=\; s_n p(s_1,\dots,s_n) + q(s_1,\dots,s_{n-1})\\ &=\; (t_n p + q)(s_1,\dots,s_n)\end{aligned}$$

Thus $g(t_1,\dots,t_n) := t_n p(t_1,\dots,t_n) + q(t_1,\dots,t_{n-1})$ does the trick and the estimation of the weighted degree of g also remains true, as we can compute

$$\begin{aligned}\mathrm{wgt}(g) \;&\le\; \max\{\,\mathrm{wgt}(t_n p),\,\mathrm{wgt}(q)\,\}\\ &\le\; \max\{\,n + \mathrm{wgt}(p),\,\mathrm{wgt}(q)\,\} \;\le\; \deg(s)\end{aligned}$$

(iv) Using (7.66.(iii)) we can compare the coefficients of the two representations of f and thereby obtain an identity for any $k \in 1\dots n$

$$a_k \;=\; (-1)^k s_k(x_1,\dots,x_d)$$

where $s_k = s_k^{(d)}$ is the elementary symmetric polynomial of degree d of $R[t_1,\dots,t_d]$. And since s is symmetric, there is a polynomial $g \in R[t_1,\dots,t_d]$ generating s via $s = g(s_1,\dots,s_d)$. Evaluating s on the roots $x_1,\dots,x_d$ then yields

$$\begin{aligned} s(x_1,\dots,x_d) &= g(s_1(x_1,\dots,x_d),\dots,s_d(x_1,\dots,x_d)) \\ &= g(-a_1,+a_2,\dots,(-1)^d a_d) \end{aligned}$$

Thus if we define $h(t_1,\dots,t_d) := g(-t_1,+t_2,\dots,(-1)^d t_d)$ we have obviously found the polynomial whose existence has been claimed.

□

Proof of (7.68):
Let us first prove that the symmetrization of any polynomial f truly is symmetric again. That is we have to check $\varrho = f_{\text{sym}} = f_{\text{sym}}$ for any permutation $\varrho \in S_n$. The idea of course is, that $\varrho S_n = \{\, \varrho\sigma \mid \sigma \in S_n \,\} = S_n$ again, as S_n is a group. Using this it is easy to compute

$$\begin{aligned} \varrho f_{\text{sym}} &= \varrho\left(\frac{1}{n!}\sum_{\sigma\in S_n}\sigma f\right) = \frac{1}{n!}\sum_{\sigma\in S_n}\varrho\,\sigma f \\ &= \frac{1}{n!}\sum_{\pi\in\varrho S_n}\pi f = \frac{1}{n!}\sum_{\pi\in S_n}\pi f = f_{\text{sym}} \end{aligned}$$

That is f_{sym} is symmetric and in particular, if $f = f_{\text{sym}}$ then f has to be symmetric. Conversely, if f is symmetric, then $\sigma f = f$ for any $\sigma \in S_n$ hence the sum in f_{sym} consists of $\#S_n$ times f. Yet $\#S_n = n!$ such that the factor in front cancels $\#S_n$, in effect only $f_{\text{sym}} = f$ remains.

Analogously we will prove that f_{asym} is antisymmetric. That is we have to check $\varrho = f_{\text{sym}} = \text{sgn}(\varrho) f_{\text{sym}}$ for any permutation $\varrho \in S_n$. Again we use $\varrho S_n = S_n$ and also $\text{sgn}(\sigma) = \text{sgn}(\varrho)^2\text{sgn}(\sigma) = \text{sgn}(\varrho)\text{sgn}(\varrho\sigma)$ to compute

$$\begin{aligned} \varrho f_{\text{asym}} &= \varrho\left(\frac{1}{n!}\sum_{\sigma\in S_n}\text{sgn}(\sigma)\sigma f\right) = \frac{1}{n!}\sum_{\sigma\in S_n}\text{sgn}(\sigma)\varrho\,\sigma f \\ &= \frac{1}{n!}\sum_{\pi\in\varrho S_n}\text{sgn}(\sigma)\pi f = \frac{1}{n!}\sum_{\pi\in\varrho S_n}\text{sgn}(\varrho)\text{sgn}(\pi)\pi f \\ &= \text{sgn}(\varrho)\,\frac{1}{n!}\sum_{\pi\in S_n}\text{sgn}(\pi)\pi f = \text{sgn}(\varrho) f_{\text{asym}} \end{aligned}$$

That is f_{asym} is symmetric and in particular, if $f = f_{\text{asym}}$ then f has to be anti-symmetric. Conversely, if f is anti-symmetric, then $\sigma f = \text{sgn}(\sigma) f$ such that in each summand $\text{sgn}(\sigma)^2 = 1$ vanishes and the sum in f_{asym} runs over $\#S_n$ times f. Again, $\#S_n = n!$ such that the factor in front cancels $\#S_n$, in effect only $f_{\text{asym}} = f$ remains. □

Proof of (1.49):

(i) We first prove the uniqueness of c and h: Suppose the identity in the claim holds true, then

multiplying this equation with $(t-x)^k g(t)$ yields

$$cg(t) + h(t)(t-x) \;=\; f(t)$$

This is an equation in the polynomial ring $E[t]$, if we evaluate both sides in x the right-hand side is reduced to $cg(x)$, as $(t-x)(x) = 0$. Therefore $cg(x) = f(x)$ such that we get $c = f(x)g(x)^{-1}$ and thereby also $h(t) = (f(t) - cg(t))/(t-x)$ is determined uniquely. Thus it only remains to prove that such c and h truly exist. If we define $c := f(x)g(x)^{-1} \in E$ then it is clear that

$$\Big(f(t) - cg(t)\Big)(x) \;=\; 0$$

And as x is a root of $f(t) - cg(t)$ by (7.54.(iii)) $t - x$ is a divisor, that is there is a polynomial $h \in E[t]$ such that $h(t)(t-x) = f(t) - cg(t)$. And if we divide this equality by $(t-x)^k g(t)$ in $E(t)$ then we get the equality (almost) as in the claim

$$\frac{h(t)}{(t-x)^{k-1}g(t)} \;=\; \frac{f(t) - cg(t)}{(t-x)^k g(t)} \;=\; \frac{f(t)}{(t-x)^k} - \frac{cg(t)}{(t-x)^k g(t)}$$

(ii) We obviously use induction on the number r of distinct roots of g. In the case $r = 1$ we use a second induction on $k = k_1$. In the case $k = 1$ we have $g = b(t-x)$ and since $\deg(f) < \deg(g) = 1$ we see that f is constant $c = f \in E$ already - thus $f(t)/g(t) = c/b(t-x)$ is established. Now consider the induction step $k \mapsto k+1$, here we apply (i) with $g(t) = b$ to get

$$\frac{f(t)}{g(t)} \;=\; \frac{f(t)}{(t-x)^{k+1}b} \;=\; \frac{c}{(t-x)^{k+1}} + \frac{h(t)}{(t-x)^k b}$$

Hereby $c = f(x)g(x)^{-1} = f(x)b^{-1}$ and $h(t) = (f(t) - cb)/(t-x)$. From the explicit description of h we get $\deg(h) = \deg(f) - 1 < \deg(g) - 1 = k$. Thus we may apply the induction hypothesis to $h(t)/b(t-x)^k$ obtaining the claim in the case $r = 1$:

$$\frac{f(t)}{g(t)} \;=\; \frac{c}{(t-x)^{k+1}} + \frac{h(t)}{b(t-x)^k} \;=\; \frac{c}{(t-x)^{k+1}} + \sum_{j=1}^{k} \frac{c_j}{(t-x)^j}$$

So we are now concerned with the induction step $r \mapsto r+1$: To do this we abbreviate $k := k_{r+1}$ and $x := x_{r+1}$ and let $q(t) := b(t-x_1)^{k_1} \dots (t-x_r)^{k_r}$. Then g can be written as $g(t) = (t-x)^k q(t)$ and $q(x) \neq 0$, so we are in the position to apply (i) again, this time with $g(t) = q(t)$

$$\frac{f(t)}{g(t)} \;=\; \frac{f(t)}{(t-x)^k q(t)} \;=\; \frac{c}{(t-x)^k} + \frac{h(t)}{(t-x)^{k-1}q(t)}$$

Thereby $c = f(x)q(x)^{-1}$ again and $h(t)$ is given to be $h(t) = (f(t) - cq(t))/(t-x)$ and as both $\deg(q) = \deg(g) - k < \deg(g)$ and $\deg(f) < \deg(g)$ we find $\deg(f(t) - cq(t)) < \deg(g)$ and hence

$$\deg(h) \;<\; \deg(g) - 1 \;=\; \deg\Big((t-x)^{k-1}q\Big)$$

Hence the induction hypothesis may be applied to $h(t)/(t-x)^{k-1}q(t)$ again such that we can also

conclude this induction step, by replacing $h(t)$

$$\frac{f(t)}{g(t)} \;=\; \frac{c}{(t-x)^k} + \sum_{i=1}^{r}\sum_{j=1}^{k_i}\frac{c_{i,j}}{(t-x_i)^j} + \sum_{j=1}^{k-1}\frac{c_{r+1,j}}{(t-x)^j}$$

□

Proof of (7.23):

(i) Consider any polynomial $f \in R[t_i \mid i \in I]$, by definition f only has finitely many non-zero coefficients $f[\alpha] \neq 0$, where $\alpha = (\alpha_i) \in \mathbb{N}^{\oplus I}$. Likewise any α only has finitely many non-zero entries. That is $I(\alpha) := \{\, i \in I \mid \alpha_i \neq 0 \,\} \in \Omega(I)$ is a finite set and as

$$I(f) \;\subseteq\; \bigcup \Big\{\, I(\alpha) \mid \alpha \in \mathbb{N}^{\oplus I}, f[\alpha] \neq 0 \,\Big\}$$

is a finite union of finite sets, we see that $I(f) \in \Omega(I)$ is a finite set. Also, for any α with $f[\alpha] \neq 0$, we get $I(\alpha) \subseteq I(f)$. But from this it is clear, that f is contained in R_ω, where $\omega := I(f)$, as

$$f \;=\; \sum_{\alpha\in\mathbb{N}^{\oplus I}} f[\alpha]\, t^\alpha \;=\; \sum_{\alpha\in I(f) f[\alpha]\, \prod_{i\in I(\alpha)}} t_i^{\alpha_i} \;\in\; R[t_i \mid i \in I(f)]$$

As f was an arbitrary polynomial, we see that the entire polynomial ring is contained in the union of the finitely generated polynomial rings $R[t_i \mid i \in \omega]$.

(ii) By construction of polynomial rings $R[t_1,\ldots,t_n]$ has the basis $\{\, t^\alpha \mid \alpha \in \mathbb{N}^n \,\}$ as an R-module. And for some $f \in R[t_1,\ldots,t_n]$ the inclusion $f \in R[t_1,\ldots,t_j]$ means that

$$\forall\, \alpha = (\alpha_1,\ldots,\alpha_n) \in \mathbb{N} \;:\; \big(\exists\, k \in j+1\ldots n \;:\; \alpha_k > 0 \;\Longrightarrow\; f[\alpha] = 0\big)$$

Likewise $f \in R[t_i,\ldots,t_n]$ means $f[\alpha] = 0$ for any $\alpha \in \mathbb{N}^n$ that features some $k \in 1\ldots i-1$ whith $\alpha_k > 0$. Now take a look at any $f \in R[t_1,\ldots,t_n]$ in this basis representation

$$f \;=\; \sum_{\alpha\in\mathbb{N}^n} f[\alpha]\, t^\alpha$$

If $f \in R[t_1,\ldots,t_j] \cap R[t_i,\ldots,t_n]$ then we can omit all $\alpha = (\alpha_1,\ldots,\alpha_n) \in \mathbb{N}^n$ with $\alpha_k > 0$ for some $k \in \{\, 1,\ldots,i-1,j,\ldots,n \,\}$. That is there only remain those $f[\alpha]$ that belong to some α for which we get $\alpha_k > 0 \;\Longrightarrow\; k \in i\ldots j$. And then f clearly is an element of

$$f \;=\; \sum_{(\alpha_i,\ldots,\alpha_j)\in\mathbb{N}^{j-i+1}} f[\alpha]\, t^\alpha \;\in\; R[t_i,\ldots,t_j]$$

By the same reasoning such an f is contained in the intersection $R[t_1,\ldots,t_j] \cap R[t_i,\ldots,t_n]$. In particular, if $j < i$ then $i\ldots j = \emptyset$. That is the only $\alpha \in \mathbb{N}^n$ for which $f[\alpha] \neq 0$ is allowed is $\alpha = 0$. And this means $f = f[\alpha]\,\mathbf{1} \in R$ is a constant polynomial (and vice versa).

(iii) It is obvious that ε is surjective, additive $\varepsilon(f+g) = \varepsilon(f) + \varepsilon(g)$, linear $\varepsilon(a\,f) = a\,\varepsilon(f)$ and unital $\varepsilon(\mathbf{1}) = 1$. The only non-obvious part is the multiplicativity, thus let $f, g \in R[\![t_i \mid i \in I]\!]$ and

compute

$$\begin{aligned}\varepsilon(f\,g) &= \varepsilon\left(\sum_{\gamma}\sum_{\alpha+\beta=\gamma} f[\alpha]\,g[\beta]\,t^{\gamma}\right)\\ &= \sum_{\alpha+\beta=0} f[\alpha]\,g[\beta] \;=\; f[0]\,g[0] \;=\; \varepsilon(f)\,\varepsilon(g)\end{aligned}$$

(iv) Clearly $\mathbb{N}^{n+1} = \mathbb{N}^n \times \mathbb{N}$ is a product of the commutative monoids $\mathbb{N}^n$ and $\mathbb{N}$. Therefore the claim is just a special case of (7.12.(vi)).

(iv) Clearly Φ_a is bijective, as the inverse mapping is given by $\Phi_a^{-1} = \Phi_{-a}$. Further it is obvious that Φ_a is additive $\Phi_a(f+g) = \Phi_a(f) + \Phi_a(g)$, linear $\Phi_a(\lambda\, f) = \lambda\, \Phi_a(f)$ and unital $\Phi_a(\mathbf{1}) = \mathbf{1}$. Thus it only remains to verify the multiplicativety of Φ_a. Choose any $f, g \in R[t_1, \ldots, t_n]$ and compute

$$\begin{aligned}\Phi_a(f\,g) &= \Phi_a\left(\sum_{\gamma}\sum_{\alpha+\beta=\gamma} f[\alpha]\,g[\beta]\,t^{\gamma}\right)\\ &= \sum_{\gamma}\sum_{\alpha+\beta=\gamma} f[\alpha]\,g[\beta]\,(t+a)^{\gamma}\\ &= \left(\sum_{\alpha} f[\alpha]\,(t+a)^{\alpha}\right)\left(\sum_{\beta} g[\beta]\,(t+a)^{\beta}\right)\\ &= \Phi_a(f)\,\Phi_a(g)\end{aligned}$$

(vi) We will prove this by induction on n: For the case $n = 1$ we use division with remainder (2.67) of f by $t_1 - a_1$ to write f in the form $f(t_1) = q(t_1)(t_1 - a_1) + r(t_1)$. Thereby $r = 0$ or $\deg(r) < \deg(t_1 - a_1) = 1$ such that $\deg(r) = 0$. That is $r(t_1) = r\mathbf{1}$ for some $r \in R$, possibly $r = 0$. Let us now evaluate $f(t_1)$ in a_1 here we find

$$f(a_1) \;=\; q(a_1)(a_1 - a_1) + r(a_1) \;=\; q(a_1)\cdot 0 + r \;=\; r$$

That is we have $f(t_1) = q(t_1)(t_1 - a_1) + r = q(t_1)(t_1 - a_1) + f(a_1)$ and this is precisely the claim in the case $n = 1$. For the induction step we consider $f \in R[t_1, \ldots, t_n, t_{n+1}]$ and let $S := R[t_1, \ldots, t_n]$. By the isomprphism in (iii) we may write $f(t_1, \ldots, t_n, t_{n+1}) \in S[t_{n+1}]$. Let us now consider any $a_{n+1} \in R \subseteq S$. As in the case $n = 1$ we may write

$$f(t_1, \ldots, t_n, t_{n+1}) \;=\; q_{n+1}(t_1, \ldots, t_n, t_{n+1})\big(t_{n+1} - a_{n+1}\big) + f(t_1, \ldots, t_n, a_{n+1})$$

for some $q_{n+1} \in S[t_{n+1}] = R[t_1, \ldots, t_n, t_{n+1}]$. However we clearly have $f(t_1, \ldots, t_n, a_{n+1}) \in S$ and hence we may use the induction hypothesis to write this polynomial in the form

$$f(t_1, \ldots, t_n, a_{n+1}) \;=\; \sum_{k=1}^{n} q_k(t_1, \ldots, t_k)\big(t_k - a_k\big) + f(a_1, \ldots, a_n, a_{n+1})$$

If we combine these two equations, the equation of the induction step becomes readily apparent, so we may conclude our proof of (v) with the following equations

$$f(t_1, \ldots, t_n, t_{n+1}) \;=\; q_{n+1}(t_1, \ldots, t_n, t_{n+1})\big(t_{n+1} - a_{n+1}\big)$$

$$
\begin{aligned}
&\quad + \sum_{k=1}^{n} q_k(t_1,\dots,t_k)\big(t_k - a_k\big) + f(a_1,\dots,a_n,a_{n+1}) \\
&= \sum_{k=1}^{n+1} q_k(t_1,\dots,t_k)\big(t_k - a_k\big) + f(a_1,\dots,a_n,a_{n+1})
\end{aligned}
$$

(vii) Because of the isomorphism in (iv) it suffices to check the case $n = 1$. If now $a \in R^*$ is a unit of R it is clear that $a\mathbf{1} \in R[t]^*$ is a unit of $R[t]$, since $(a\mathbf{1})^{-1} = a^{-1}\mathbf{1}$. In the converse direction we fix the standard order $\leq$ on $\mathbb{N}$ which clearly is a monomial well-ordering. If now $f \in R[t]^*$ is a unit of $R[t]$ then by definition there is some $g \in R[t]$ such that $fg = \mathbf{1}$. Thus we may evaluate the degrees to find that

$$
0 \;=\; \deg(\mathbf{1}) \;=\; \deg(f\,g) \;=\; \deg(f) + \deg(g)
$$

This of course implies $\deg(f) = 0 = \deg(g)$, i.e. f and g are constant polynomials $f = a\mathbf{1}$ and $g = b\mathbf{1}$. But now it is obvious that $b = a^{-1}$ and hence a truly is an invertible element of R.

(viii) Because of isomorphism in (iv) it suffices to check the case $n = 1$ again. We first assume that $f \in R[\![t]\!]^*$ is an invertible element of $R[\![t]\!]$. By definition this means that there is some $g \in R[\![t]\!]$ such that $fg = \mathbf{1}$. We now apply the epimorphism in (ii) to find that $f[0]$ truly is an invertible element of R

$$
1 \;=\; \varepsilon(\mathbf{1}) \;=\; \varepsilon(f\,g) \;=\; \varepsilon(f)\,\varepsilon(g) \;=\; f[0]\,g[0]
$$

In the converse direction we define g as in the remark above, i.e. we let $g[0] := f[0]^{-1}$ and recursively $g[k] := -f[0]^{-1} \sum_{i=0}^{k-1} f[n-i]\,g[i]$. By the construction it is clear that $fg[0] = f[0]g[0] = 1$. We will now prove that $fg = \mathbf{1}$, i.e. $fg[k] = 0$ for any $k \in \mathbb{N}$. To do this we use induction on k and compute

$$
\begin{aligned}
fg[1] &= f[0]\,g[1] + f[1]\,g[0] \\
&= -f[1]\,g[0] + f[1]\,g[0] \;=\; 0 \\
fg[k] &= \sum_{i=0}^{k} f[k-i]\,g[i] \\
&= \sum_{i=0}^{k-1} f[k-i]\,g[i] + f[0]\,g[k] \\
&= \sum_{i=0}^{k-1} f[k-i]\,g[i] - \sum_{i=0}^{k-1} f[k-i]\,g[i] \;=\; 0
\end{aligned}
$$

□

Proof of (7.18):

The proofs of all these statements are straightforward computations. The statements for the sum $f+g$ are simple and the proofs of the statements for the product fg follow the same lines as the proof of $R[t \mid A]$ being an integral domain. Thus we introduce the following notation again: Consider $0 \neq f, g \in R[t \mid A]$ any two non-zero polynomials and denote the coefficients on which f and g are non-zero by

$$
\{\,\alpha_1,\dots,\alpha_m\,\} \;:=\; \{\,\alpha \in A \mid f[\alpha] \neq 0\,\}
$$

$$\{\,\beta_1,\ldots,\beta_n\,\} \;:=\; \{\,\beta\in A \mid g[\beta]\neq 0\,\}$$

Without loss of generality we may assume $\alpha_1<\cdots<\alpha_m$ and likewise $\beta_1<\cdots<\beta_n$. Then this will enable us to prove the above assertions (for a general commutative ring R) easily:

- By definition we immediately get $\mathrm{lt}(f)=f[\alpha_m]\,t^{\alpha_m}=\mathrm{lc}(f)\,\mathrm{lm}(f)$.
- If $\max\{\,\alpha_m,\beta_n\,\}<\gamma$ then $f[\gamma]=0=g[\gamma]$ and hence $f[\gamma]+g[\gamma]=0$ as well. But this already proves $\deg(f+g)\leq\max\{\,\deg(f),\deg(g)\,\}$.
- If $\alpha_m+\beta_n<\gamma$ then for any $i\in 1\ldots m$ and $j\in 1\ldots n$ we obtain $\alpha_i+\beta_j\leq\alpha_m+\beta_j\leq\alpha_m+\beta_n<\gamma$. Hence there are no non-zero coefficients $f[\alpha_i]\neq 0$ and $g[\beta_j]\neq 0$ such that $\alpha_i+\beta_j=\gamma$. But for the coefficient $fg\,[\gamma]$ of the product fg this implies $fg[\gamma]=0$, as at least one $f[\alpha_i]$ or $g[\beta_j]$ has to be 0. And hence $\deg(f\cdot g)\leq\deg(f)+\deg(g)$, as

$$fg[\gamma] \;=\; \sum_{\alpha+\beta=\gamma} f[\alpha_i]\,g[\beta] \;=\; \sum_{\alpha_i+\beta_j=\gamma} f[\alpha_i]\,g[\beta_j] \;=\; 0$$

In the following we assume that R is an integral domain and A is integral, too. As $\leq$ is a positive order on A and A is integral $(A,+,\leq)$ is a strictly positively ordered monoid, by (7.6.(iii)). Then we are able to prove the even stronger statements:

- Let $\gamma:=\alpha_m+\beta_n$, then for any $i\in 1\ldots m$ and $j\in 1\ldots n$ we find that $\alpha_i+\beta_j=\gamma$ is equivalent, to $i=m$ and $j=n$, due to (7.6.(iv)). But for the coefficient $fg\,[\gamma]$ of the product fg this again implies

$$\sum_{\alpha+\beta=\gamma} f[\alpha_i]\,g[\beta] \;=\; \sum_{\alpha_i+\beta_j=\gamma} f[\alpha_i]\,g[\beta_j] \;=\; f[\alpha_m]\,g[\beta_n]$$

 But as R is an integral domain, we conclude that $f[\alpha_m]\,g[\beta_n]\neq 0$ is non-zero again and therefore $\deg(f\cdot g)\geq\deg(f)+\deg(g)$. But as $\deg(f\cdot g)\leq\deg(f)+\deg(g)$ is true in general, we conclude that $f[\alpha_m]\,g[\beta_n]\neq 0$ implies $\deg(f\cdot g)=\deg(f)+\deg(g)$.
- As we have seen $\gamma:=\deg(f\cdot g)=\deg(f)+\deg(g)=\alpha_m+\beta_n$ we immediately get $\mathrm{lm}(f\cdot g)=t^{\gamma}=t^{\alpha_m+\beta_n}=t^{\alpha_m}\cdot t^{\beta_n}=\mathrm{lt}(f)\cdot\mathrm{lt}(g)$ and likewise $\mathrm{lc}(f\cdot g)=fg\,[\gamma]=f[\alpha_m]\,g[\beta_n]=\mathrm{lc}(f)\cdot\mathrm{lc}(g)$. But of course this includes $\mathrm{lt}(f\cdot g)=\mathrm{lt}(f)\cdot\mathrm{lt}(g)$, as this is immediate from $\mathrm{lt}(f\cdot g)=\mathrm{lc}(f\cdot g)\,\mathrm{lm}(f\cdot g)=\mathrm{lc}(f)\cdot\mathrm{lc}(g)\,\mathrm{lm}(f)\cdot\mathrm{lm}(g)=\mathrm{lc}(f)\,\mathrm{lm}(f)\cdot\mathrm{lc}(g)\,\mathrm{lm}(g)=\mathrm{lt}(f)\cdot\mathrm{lt}(g)$.
- Nota even if R is no integral domain, but f is monic we have $f[\alpha_m]=1$ and hence $f[\alpha_m]\,g[\beta_n]=g[\beta_n]\neq 0$. Analogously the same is true, if g is monic. But from this we found $\deg(f\cdot g)=\deg(f)+\deg(g)$. And from this property all the following three identities were inferred.

□

Proof of (7.26):

(i) If $a=0$, then $at^{\alpha}=0$ is the zero-polynomial and hence $\deg_\omega(0)=-\infty$ by definition. And if $a\neq 0$ then the only (and hence maximal) $\beta\in\mathbb{N}^n$ with $at^{\alpha}[\beta]\neq 0$ is $\beta=\alpha$ such that $\deg_\omega(at^{\alpha})=|\alpha|_\omega$.

(ii) Consider any non-zero polynomial $0\neq f\in R[t_1,\ldots,t_n]$ then compute

$$\deg_\omega(f) \;=\; \max\{\,|\alpha|_\omega \mid \alpha\in\mathbb{N}^n, f[\alpha]\neq 0\,\}$$

$$\begin{aligned} &= \max\{\, \deg_\omega(f[\alpha]t^\alpha) \mid \alpha \in \mathbb{N}^n, f[\alpha] \neq 0 \,\} \\ &= \max\{\, \deg_\omega(f[\alpha]t^\alpha) \mid \alpha \in \mathbb{N}^n \,\} \end{aligned}$$

(iii) and (iv) can be treated simultaneously. We fix the ω-graded lexicographic order on $\mathbb{N}^n$ and denote it by $\leq := \leq_{\text{lex}}$. Then we already know that $(\mathbb{N}^n, +, \leq)$ is a positively (even algebraically) ordered monoid and by construction of $\leq$ for any polynomial $f \in R[t_1, \ldots, t_n]$

$$\begin{aligned} \deg_\omega(f) &= \max\{\, |\alpha|_\omega \mid f[\alpha] \neq 0 \,\} \\ &= |\max_{\leq}\{\, \alpha \mid f[\alpha] \neq 0 \,\}|_\omega \\ &= |\deg_{\leq}(f)|_\omega \end{aligned}$$

But for $\deg_{\leq}$ the claims have already been proved in (7.18) and hence we get

$$\begin{aligned} \deg_\omega(f+g) &= |\deg_{\leq}(f+g)|_\omega \\ &\leq |\max_{\leq}\{\, \deg_{\leq}(f), \deg_{\leq}(g) \,\}|_\omega \\ &= \max\{\, |\deg_{\leq}(f)|_\omega, |\deg_{\leq}(g)|_\omega \,\} \\ &= \max\{\, \deg_\omega(f), \deg_\omega(g) \,\} \end{aligned}$$

$$\begin{aligned} \deg_\omega(f \cdot g) &= |\deg_{\leq}(f \cdot g)|_\omega \\ &\leq |\deg_{\leq}(f) + \deg_{\leq}(g)|_\omega \\ &= |\deg_{\leq}(f)|_\omega + |\deg_{\leq}(g)|_\omega \\ &= \deg_\omega(f) + \deg_\omega(g) \end{aligned}$$

□

Proof of (7.22):
Let us abbreviate $A := R[t_i \mid i \in I]$ and $B := R[t_j \mid j \in J]$. The embedding $A \hookrightarrow B$ has already been proved in (7.12.(iii)). In particular if f and $g \in A$, then $fg \in A$ again. Conversely consider $0 \neq f, g \in B$ such that $fg \in A$. For any $j \in J$ let us define

$$\deg_j(f) := \begin{cases} \max\{\, \alpha_j \mid \alpha \in \mathbb{N}^{\oplus J},\, f[\alpha] \neq 0 \,\} & \text{for } f \neq 0 \\ -\infty & \text{for } f = 0 \end{cases}$$

Note that this is the degree in the polynomial ring $S[t_j]$ where S denotes the integral domain $S := R[t_i \mid i \in J \setminus j]$. This is legitimate, since $B \cong_{\mathsf{a}} S[t_j]$ according to (7.12.(vi)) - you may also want to compare (7.23.(iii)). Then by construction of the embedding we have $f \in R[t_i \mid i \in I]$ if and only if $\deg_j(f) = 0$ for any $j \in J \setminus I$. And as S is an integral domain we have

$$0 = \deg_j(fg) = \deg_j(f) + \deg_j(g)$$

for any $j \in J \setminus I$. As both $\deg_j(f)$ and $\deg_j(g) \in \mathbb{N}$ their sum can only be zero, if $\deg_j(f) = 0 = \deg_j(g)$ such that f and $g \in A$. □

Proof of (7.28):
Let us prove the claim by induction on n: In case $n = 1$ we are given a polynomial $f \in R[t_1]$, let $d := \deg(f)$ be its degree, then we can write f in the following form

$$f \;=\; \sum_{i=0}^{d} f[i]\, t_1^i \;=\; f(0) + \sum_{i=1}^{d} f[i]\, t_1^i \;=\; f(0) + t_i \sum_{i=0}^{d-1} f[i+1]\, t_1^i$$

That is we may take $f_1 = \sum_i f[i+1] t_1^i$ which is a polynomial in $R[t_1]$ of degree $\deg(f_1) = d - 1 < d = \deg(f)$. So we can commence with the induction step $n+1$: That is we are given a polynomial $f \in R[t_1, \ldots, t_{n+1}]$ and let $d := \deg_{n+1}(f)$. We can then we write f, as

$$f \;=\; \sum_{\alpha \in \mathbb{N}^n} \sum_{i=0}^{d} f[\alpha, i]\, t^\alpha t_{n+1}^i$$

Let us split this sum into a part with $i = \alpha_{n+1} = 0$ and a part with $i = \alpha_{n+1} \geq 1$. Then we can pull out t_{n+1} once (as above) to arrive at the following expression

$$f \;=\; \sum_{\alpha \in \mathbb{N}^n} f[\alpha, 0]\, t^\alpha + \left(\sum_{i=0}^{d-1} f[\alpha, i+1]\, t^\alpha t_{n+1}^i \right) t_{n+1}$$

The term in brackets is $f_{n+1} \in R[t_1, \ldots, t_{n+1}]$. From its explicit representation we find $\deg(f_{n+1}) = \deg(f) - 1 < \deg(f)$ again. That is f_{n+1} satisfies properties (1) and (2) of the claim. And the term in front is a polynomial in $R[t_1, \ldots, t_n]$ only. Thus by induction hypothesis it is of the form $f(0) + \sum_k f_k(t_1, \ldots, t_k) t_k$ for some polynomials f_k satisfying properties (1) and (2). Altogether we have found

$$f \;=\; f(0) + \sum_{k=1}^{n} f_k(t_1, \ldots, t_k) t_k + f_{n+1}(t_1, \ldots, t_{n+1}) t_{n+1}$$

Thus $f \in R[t_1, \ldots, t_{n+1}]$ can be written in the form given in the claim, again. And as all the f_k for $k \in 1 \ldots n+1$ satisfy the properties (1) and (2) we have completed the induction step. □

Proof of (3.43):

(i) If $f \in \mathfrak{a}R[t]$ then by (3.40.(i)) f is of the form $f = a_1 f_1 + \cdots + a_n f_n$ for some $a_i \in \mathfrak{a}$ and $f_i \in R[t]$. Thereby for any $k \in \mathbb{N}$ the k-th coefficient of f is given to be $f[k] = a_1 f_1[k] + \cdots + a_n f_n[k] \in \mathfrak{a}$ and hence $f \in \mathfrak{a}[t]$. Conversely if $f \in \mathfrak{a}[t]$ is of degree $d := \deg(f)$, then f is also is in $\mathfrak{a}R[t]$, as

$$f \;=\; \sum_{k=0}^{d} f[k] t^k \;\in\; \sum_{k=0}^{d} \mathfrak{a}R[t] \;=\; \mathfrak{a}R[t]$$

(ii) Clearly we obtain a surjective homomorphism of rings by extension of the canonical epimorphism $R \twoheadrightarrow R/\mathfrak{a} : b \mapsto b + \mathfrak{a}$ to the polynomial ring. That is we regard

$$\varrho \;:\; R[t] \;\twoheadrightarrow\; \left(R \Big/ \mathfrak{a} \right)[t] \;:\; f \mapsto \sum_{k=0}^{\infty} \big(f[k] + \mathfrak{a} \big) t^k$$

We now prove, that the kernel of ϱ is given to be $\mathrm{kn}(\varrho) = \mathfrak{a}[t]$. Then the isomorphism follows from the first isomorphism theorem (1.83.(ii)). If $f \in \mathfrak{a}[t]$ then $f[k] \in \mathfrak{a}$, such that $f[k] + \mathfrak{a} = 0 + \mathfrak{a}$ for

any $k \in \mathbb{N}$ and thereby $\varrho(f) = 0$. Conversely consider some $f \in R[t]$ with $\varrho(f) = 0$. That is $\varrho(f)[k] = 0$ for any $k \in \mathbb{N}$. But by definition of ϱ this is $f[k] + \mathfrak{a} = 0 + \mathfrak{a}$ and hence $f[k] \in \mathfrak{a}$. And this again means $f \in \mathfrak{a}[t]$.

- Clearly $\mathfrak{a}[t] + tR[t]$ is an ideal, as it is a sum of such. We have to check, that this is identical, to $\{ f \in R[t] \mid f(0) \in \mathfrak{a} \}$. Let us begin with some $f \in R[t]$ with $a := f(0) \in \mathfrak{a}$. That is f is of the form $f = a\mathbf{1} + tg(t)$ where $g := f[1] + f[2]t + \cdots \in R[t]$. In this form we see $f \in \mathfrak{a}[t] + tR[t]$ clearly. Conversely, if $g \in \mathfrak{a}[t] + tR[t]$ then $g = f + th$ for some $f \in \mathfrak{a}[t]$ and $h \in R[t]$. From this we see $g(0) = f(0) + 0 \cdot h(0) = f(0) = f[0] \in \mathfrak{a}$. Thus both descriptions of this ideal are identical.

- Much like the proof of the first part we start with a homomorphism of rings, that obviously is surjective: $\varrho : R[t] \to R/\mathfrak{a} : f \mapsto f(0) + \mathfrak{a}$. This time we need to show $\ker(\varrho) = \mathfrak{a}[t] + tR[t]$. If we start with $f \in R[t]$ with $0 = \varrho(f) = f(0) + \mathfrak{a}$ we see $f(0) \in \mathfrak{a}$. But then

$$f \;=\; \sum_{k=0}^{\infty} f[k]t^k \;=\; f(0) + t\sum_{k=1}^{\infty} f[k]t^{k-1} \;\in\; \mathfrak{a} + tR[t]$$

and in particular $f \in \mathfrak{a}[t] + tR[t]$. If we conversely start with $f \in \mathfrak{a}[t] + tR[t]$, then f is of the form $f = \sum_k a_k t^k + tg(t)$ for some $a_k \in \mathfrak{a}$ and $g \in R[t]$. In particular $f(0) = a_0 \in \mathfrak{a}$ and hence $\varrho(f) = 0$. That is we have both inclusions of $\ker(\varrho) = \mathfrak{a}[t] + tR[t]$ and hence we find the isomorphism in the claim by the first isomorphism theorem (1.83.(ii)), again.

(iii) If $\mathfrak{p}$ is prime then $R/\mathfrak{p}$ is an integral domain and hence the polynomial ring $(R/\mathfrak{p})[t]$ is an integral domain, too. By the first isomorphism in (ii) this means $R[t]/\mathfrak{p}[t]$ is an integral domain, as well. And this means $\mathfrak{p}[t] \trianglelefteq_{\mathrm{i}} R[t]$ is a prime ideal, by (2.12). In complete analogy: If $\mathfrak{m}$ is a maximal ideal, then $R/\mathfrak{m}$ is a field. And due to the second isomorphism in (ii) we find that $R[t]/\widetilde{\mathfrak{m}}$ is a field. And this again means, that $\widetilde{\mathfrak{m}}$ is a maximal ideal of $R[t]$.

□

Proof of (2.168):

(i) By (3.43.(i)) we have $\mathfrak{m}[t] = \mathfrak{m}\,R[t]$ and (8.15) guarantees $\mathfrak{m}\,R[t] = (\mathfrak{n} \cap R)R[t] \subseteq \mathfrak{n}$. As $\mathfrak{n}$ is a maximal ideal, by assumption we find that

$$\mathfrak{n} \Big/ \mathfrak{m}[t] \;\trianglelefteq_{\mathrm{i}}\; R[t] \Big/ \mathfrak{m}[t] \;\cong_{\mathrm{r}}\; \left(R \Big/ \mathfrak{m}\right)[t]$$

is a maximal ideal, again - where the isomorphy is due to (3.43.(ii)). By assumption $\mathfrak{m} \trianglelefteq_{\mathrm{i}} R$ is a maximal ideal and hence $E := R/\mathfrak{m}$ is a field. Then the polynomial ring $E[t]$ is a PID. Thus the image of $\mathfrak{n}/\mathfrak{m}[t]$ in $E[t]$ is a maximal ideal again and hence generated by a non-zero prime element $\overline{f} \in E[t]$. We can even choose $\overline{f}$ to be monic. The isomorphism is given to be

$$\Phi\big(f + \mathfrak{m}[t]\big) \;=\; \sum_{k=0}^{\infty} \big(f[k] + \mathfrak{m}\big)\, t^k$$

Pick up some $f \in R[t]$ such that $\Phi(f + \mathfrak{m}[t]) = \overline{f}$. As $\overline{f}$ is monic, so is f and as $\overline{f}$ is a prime

element, so is $f+\mathfrak{m}[t]$. Let us evaluate $\mathfrak{n}/\mathfrak{m}[t]$, which is the pre-image of $\overline{f}E[t]$ under Φ

$$\mathfrak{n}\Big/_{\mathfrak{m}[t]} \;=\; \Phi^{-1}\left(\overline{f}\,E[t]\right) \;=\; \big(f+\mathfrak{m}[t]\big)^{R[t]}\Big/_{\mathfrak{m}[t]} \;=\; \mathfrak{m}[t]+fR[t]\Big/_{\mathfrak{m}[t]}$$

By the correspondence theorem of ideals in quotient rings we now see that $\mathfrak{n}$ corresponds to the ideal $\mathfrak{m}[t]+fR[t]$. This is property (1) and we have already argued above, that f is monic and (2) $f+\mathfrak{m}[t]$ is a prime element.

(ii) Let $U := R\setminus\{0\}$, that is $E = U^{-1}R$ and thereby $U^{-1}R[t] := (U^{-1}R)[t] = E[t]$. By (2.132.(i)) we have an isomorphism $\Phi : U^{-1}R[t] \xrightarrow{\sim} E[t]$ given by $\Phi(f/u) = \sum_k (f[k]/u)\,t^k$. An isomorphism of rings obviously induces a one-to-one correspondence of prime ideals

$$\begin{array}{ccc} \mathrm{Spec}\big(U^{-1}R[t]\big) & \longleftrightarrow & \mathrm{Spec}\big(E[t]\big) \\ \mathfrak{v} & \mapsto & \Phi\big(\mathfrak{v}\big) \end{array}$$

And by the correspondence theorem of ideals in localisations (2.129) the spectrum of $U^{-1}R[t]$ corresponds to the set of prime ideals $\mathfrak{p}$ of $R[t]$ such that $\mathfrak{p}\cap U = \emptyset$. As $U = R\setminus\{0\}$ the latter property can be put as $\mathfrak{p}\cap R = 0$, equivalently. Thus we have found another correspondence

$$\begin{array}{ccc} \mathrm{Spec}\big(U^{-1}R[t]\big) & \longleftrightarrow & \big\{\,\mathfrak{p}\in\mathrm{Spec}\big(R[t]\big)\mid \mathfrak{p}\cap R = 0\,\big\} \\ \mathfrak{u} & \mapsto & \mathfrak{u}\cap R[t] \end{array}$$

Combining these we have a one-to-one correspondence of the spectrum of $E[t]$ and the prime ideals $\mathfrak{p}$ of $R[t]$ satisfying $\mathfrak{p}\cap R = 0$ given by $\mathfrak{u}\mapsto\Phi^{-1}(\mathfrak{u})\cap R[t]$. Let us decode this ideal

$$\Phi^{-1}(\mathfrak{u})\cap R[t] \;=\; \Big\{\, f\in R[t]\mid f/1\in\Phi^{-1}(\mathfrak{u})\,\Big\} \;=\; \{\,f\in R[t]\mid \iota(f)\in\mathfrak{u}\,\}$$

So this is the direction from left to right of the correspondence given in the claim. It remains to verify the converse direction from right to left. That is we start with a prime ideal $\mathfrak{p}\trianglelefteq_{\mathfrak{i}} R[t]$ such that $\mathfrak{p}\cap R = 0$ and have to prove that this $\mathfrak{p}$ corresponds to the ideal

$$\widetilde{\mathfrak{p}} \;:=\; \left\{ \sum_{k=0}^{\infty}\frac{f[k]}{u}t^k \;\middle|\; f\in\mathfrak{p},\, u\neq 0 \right\}$$

That is we have to show $\big\{\, f\in R[t]\mid \iota(f)\in\widetilde{\mathfrak{p}}\,\big\} = \mathfrak{p}$. If $f\in\mathfrak{p}$ then $\iota(f)\in\widetilde{\mathfrak{p}}$ is clear from the function rules of ι and Φ. And conversely if $f\in R[t]$ satisfies $\iota(f)\in\widetilde{\mathfrak{p}}$ then there are some $g\in\mathfrak{p}$ and $u\neq 0$ such that for any $k\in\mathbb{N}$ we get $f[k]/1 = g[k]/u$. That is $uf[k] = g[k]$ and hence $uf = g\in\mathfrak{p}$, as this is true for any $k\in\mathbb{N}$. As $\mathfrak{p}$ is a prime ideal this implies $u\mathbf{1}\in\mathfrak{p}$ or $f\in\mathfrak{p}$. But $u\mathbf{1}\in\mathfrak{p}$ would mean $u\in\mathfrak{p}\cap R = 0$ in contradiction to $u\neq 0$. Thus we conclude $f\in\mathfrak{p}$ and hence we have established the direction right to left of the correspondence, too.

□

Proof of (7.27):

(i) If $g = 0$ then $g(f) = 0\in R[t]$ such that $\deg(g(f)) = -\infty$. And regardless of f we also have $\deg(f)\cdot\deg(g) = -\infty$, which is equal. So let us now assume $g\neq 0$ and denote $d = \deg(f)$ and

$e := \deg(g)$. Let us first look at powers of f. By the polynomial rule, we have

$$f^k \;=\; \left(\sum_{i=0}^{d} f[i]\,t^i\right)^k \;=\; \sum_{|\alpha|=k} \binom{k}{\alpha} \prod_{i=0}^{d} f[i]^{\alpha_i} t^{i\cdot\alpha_i}$$

where the sum runs over all $\alpha = (\alpha_0, \ldots, \alpha_d) \in \mathbb{N}^{d+1}$ such that $|\alpha| = \alpha_0 + \cdots + \alpha_d = k$. Let us abbreviate $f[\alpha] := f[0]^{\alpha_0} \ldots f[d]^{\alpha_d}$ and $\omega(\alpha) := 0\cdot\alpha_0 + 1\cdot\alpha_1 + \ldots d\cdot\alpha_d$, then we use this formula to find an expression for $g(f) \in R[t]$

$$g(f) \;=\; \sum_{k=0}^{d} g[k]\, f^k \;=\; \sum_{k=0}^{d} g[k] \sum_{|\alpha|=k} \binom{k}{\alpha} f[\alpha]\, t^{\omega(\alpha)}$$

In particular, for $k = e$ and $\alpha = (0, \ldots, 0, e)$ the binomial coefficient k over α turns to 1 and $f[\alpha] = f[d]^e$ and $\omega(\alpha) = d\cdot e = \deg(f)\cdot\deg(g)$. The de-th coefficient of $g(f)$ thereby is

$$g(f)[de] \;=\; g[e]\cdot f[d]^e \;\neq\; 0$$

which is non-zero, as R is an integral domain. For any other combination (k, α) we have $\omega(\alpha) < de$, such that this truly is the leading coefficient of $g(f)$. In particular we have $\deg(g(f)) = d\cdot e$.

(ii) Let us first regard the case $n = 1$, that is $f \in R[t_1]$ and $g \in R[x]$. If $g(f) = 0$ then by (i) we have $\deg(f)\cdot\cdot(g) = \deg(g(f)) = -\infty$. But as $\deg(f) \geq 1$ this means $\deg(g) = -\infty$ and hence $g = 0$. Thus we have proved the claim, for $n = 1$.

Note that $n = 0$ is ruled out, as $\deg(f) \geq 1$ requires at least one variable. Now for general $2 \leq n \in \mathbb{N}$ there is some $i \in 1 \ldots n$ such that $\deg_i(f) \geq 1$, as we else would have $\deg(f) \leq 0$. For ease of notation we assume $i = 1$ and let $\mathfrak{a} := \langle t_2, \ldots, t_n \rangle_{\mathrm{i}}$. Then it is clear that

$$\Phi \;:\; R[t_1] \;\xrightarrow{\sim}\; R[t_1, \ldots, t_n] \Big/ \mathfrak{a} \;:\; f \mapsto f + \mathfrak{a}$$

is an isomorphism of R-algebras. As $g(f) = 0$ we also have $0 + \mathfrak{a} = g(f) + \mathfrak{a} = g(f + \mathfrak{a})$. Let us denote the preimage of $f + \mathfrak{a}$ in $R[t_1]$ by $\overline{f} := \Phi^{-1}(f + \mathfrak{a})$, that is $\overline{f} = \sum_{\alpha_1} f_\alpha(0) t_1^{\alpha_1}$ for some $f_\alpha \in R[t_2, \ldots, t_n]$. Then $\overline{f}$ is a polynomial in one variable t_1 and as $\deg_1(f) \geq 1$ we know $f \notin \mathfrak{a}$. That is $f + \mathfrak{a} \neq 0 + \mathfrak{a}$ and hence $\overline{f} \neq 0$, too. Since we also have

$$0 \;=\; \Phi^{-1}\big(g(f) + \mathfrak{a}\big) \;=\; g\big(\Phi^{-1}(f + \mathfrak{a})\big) \;=\; g(\overline{f})$$

we conclude from the case $n = 1$ that we must have had $g = 0$. That is we have proved the general claim $g(f) = 0 \implies g = 0$ and the converse implication $g = 0 \implies g(f)$ is trivial.

(iii) The element $p \in R$ is prime, if and only if the ideal $pR \trianglelefteq_{\mathrm{i}} R$ is prime. And by (2.12) this is equivalent to $S := R/pR$ being an integral domain. This again is equivalent to $S[t \mid A]$ being an integral domain, according to (7.12.(vii)). Now recall the isomorphy of (7.13)

$$A \Big/ pA \;\xrightarrow{\sim}\; S[t \mid A] \;:\; f + pA \mapsto \overline{\varrho}(f)$$

This means that $S[t \mid A]$ is an integral domain if and only if A/pA is. And as we have just argued

this is equivalent to $p \in A$ being prime.

(iv) Let us first consider the case of one variable $A = R[t]$ and some $a \in R$. Now suppose $(t-a) \mid fg$ for some $f, g \in R[t]$. That is there is some $u \in R[t]$ such that $fg(t) = u(t)(t-a)$. In particular, if we evaluate this expression in a, we find

$$f(a)g(a) \;=\; fg(a) \;=\; u(a)(a-a) \;=\; 0$$

As R is an integral domain this means $f(a) = 0$ or $g(a) = 0$. Without loss of generality we continue with the case $f(a) = 0$. Then we use (7.23.(v)) to write f as $f(t) = q(t)(t-a) + f(a) = q(t)(t-a)$. Thus we have already found $(t-a) \mid f$ in $R[t]$ and as this is true for any f, g we find $t - a \in R[t]$ to be a prime element of $R[t]$.

Generally for $t_i - a_i \in A$ we consider any $f, g \in A$, such that $(t_i - a_i) \mid fg$ again. Next we consider $fg \in S[t_i]$ as a polynomial in one variable over $S = R[t_j \mid j \in I \setminus \{i\}]$. Note that S is an integral domain again, according to (7.12.(vii)). Hence by the above $(t_i - a_i) \mid fg$ implies (without loss of generality) $(t_i - a_i) \mid f$ in $S[t_i] = A$, such that $t_i - a_i$ is prime in A.

(v) First of all t_iA is a prime ideal, as t_i is prime, according to (iii). A direct argument would be: Let $A_i := R[t_j \mid j \in I \setminus \{i\}]$, then we have an obvious isomorphism $A_i \xrightarrow{\sim} A/t_iA$ of R-algebras, by $f \mapsto f + t_iA$. But as R is an integral domain, so is A_i and hence t_iA has to be a prime ideal.

Let us now prove, that t_iA also is minimal over 0: If $\mathfrak{p} = 0$, then we are done, else choose some $g \in \mathfrak{p}$ with $g \neq 0$ and write this g as a polynomial in t_i over the ring A_i

$$g \;=\; \sum_{k=0}^{d} g_k\, t_i^k \;\in\; A_i[t_i]$$

As we have $g \in \mathfrak{p} \subseteq t_iA$ we see $g_0 = 0$. Also, for $d = \deg_i(g)$ we have $g_d \neq 0$. Now let $m \in \mathbb{N}$ be the minimal number, such that $g_m \neq 0$ As $g_0 = 0$ we have $m \in 1 \ldots d$. As $g_0 = \cdots = g_{m-1} = 0$ we can write g as $g = t_i^m f$ for $f = g_m + \cdots + g_d t_i^{d-m}$ and thereby

$$t_i^m f \;=\; g \;\in\; \mathfrak{p} \;\subseteq\; t_iA$$

As $\mathfrak{p}$ is prime and $m \geq 1$ we conclude $t_i \in \mathfrak{p}$ or $f \in \mathfrak{p}$. Suppose $f \in \mathfrak{p}$ was true, as $\mathfrak{p} \subseteq t_iA$ this would mean $0 + t_iA = f + t_iA = g_m + t_iA$ which is untrue, as $0 \neq g_m \in A_i$. So it must be $t_i \in \mathfrak{p}$, which is $t_iA \subseteq \mathfrak{p} \subseteq t_iA$ such that $\mathfrak{p} = t_iA$, as claimed.

□

Proof of (2.7):

(i) Let us regard the evaluation homomorphism $\varepsilon_a : F[t] \twoheadrightarrow F : f \mapsto f(a)$. As $f(a) = 0$ and $(t - a\mathbf{1}) \mid f$ are equivalent, according to (7.54.(iii)), we find

$$\mathrm{kn}(\varepsilon_a) \;=\; (t - a\mathbf{1})F[t]$$

But as ε_a is surjective the first isomorphism theorem (1.83.(ii)) tells us, that it induces an isomorphism of the form $F[t]/\mathrm{kn}(\varepsilon_a) \xrightarrow{\sim} F : f + \mathrm{kn}(\varepsilon_a) \mapsto f(a)$. As F is a field, so is $F[t]/\mathrm{kn}(\varepsilon_a)$ and this

again means, that $\mathrm{kn}(\varepsilon_a) = (t - a\mathbf{1})F[t]$ is a maximal ideal. Hence the map $a \mapsto (t - a\mathbf{1})F[t]$ is well-defined. It remains to show, that it also is injective: Suppose $(t - a\mathbf{1})F[t] = (t - b\mathbf{1})F[t]$ for some $a, b \in F$. Then we have $t - b\mathbf{1} \in (t - a\mathbf{1})F[t]$ which is $t - b\mathbf{1} = g(t) \cdot (t - a\mathbf{1})$. In particular $1 = \deg(g) + 1$ such that $\deg(g) = 0$. This again means $g = u\mathbf{1}$ for some $u \in F$. But then again $t - b\mathbf{1} = u\mathbf{1} \cdot (t - a\mathbf{1}) = ut - ua\mathbf{1}$. Comparing the coefficient in front of t we find $u = 1$ and hence $t - a\mathbf{1} = t - b\mathbf{1}$. Comparing the coefficients in front of $\mathbf{1}$ we also find $a = b$.

(ii) If $j \in \mathrm{JAC}(F[t])$ then by (2.8) using $a = 1$, we get $\mathbf{1} - j \in F[t]^*$. But by (7.23.(vii)) this means $\mathbf{1} - j = a\mathbf{1}$ for some $a \in F^*$. This again is $j = (1 - a)\mathbf{1}$. Now $tF[t]$ is a maximal ideal of $F[t]$, by (i) and as j is contained in *any* maximal ideal we in particular have $j \in tF[t]$. That is $j = g(t) \cdot t$ for some $g \in F[t]$ and thereby $j = 0$ or $0 = \deg(j) = \deg(g) + 1$. The latter is absurd, as $\deg(g)$ would have to be negative (which is $g = 0$) such that we get $j = 0$.

(iii) By the correspondence theorem of ideals (1.66), the ideals of $\mathbb{Z}_n$ are of the for $m\mathbb{Z}/n\mathbb{Z}$ for some $n\mathbb{Z} \subseteq m\mathbb{Z}$. The latter is $m \mid n$ and by the third isomorphism theorem (1.83.(iv)) we have

$$\mathbb{Z}/n\mathbb{Z} \Big/ m\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mathbb{Z} \Big/ m\mathbb{Z} \;:\; (a + n\mathbb{Z}) + m\mathbb{Z} \Big/ n\mathbb{Z} \mapsto a + m\mathbb{Z}$$

Therefore $m\mathbb{Z}/n\mathbb{Z}$ is maximal if and only if $\mathbb{Z}_m$ is a field and this is the case iff m is prime. As $m \mid n$ this leaves $m \in \{ p_1, \ldots, p_r \}$, that is the maximal ideals of $\mathbb{Z}_n$ are the $p_i\mathbb{Z}/n\mathbb{Z}$ for $i \in 1 \ldots r$. Let $q := p_1 \ldots p_r$ then $q\mathbb{Z}/n\mathbb{Z}$ is contained in any $p_i\mathbb{Z}/n\mathbb{Z}$. Conversely if $a + n\mathbb{Z} \in \mathrm{JAC}(\mathbb{Z}_n)$ then $a + n\mathbb{Z} \in p_i\mathbb{Z}/n\mathbb{Z}$ means $a \in p_i\mathbb{Z}$ which is $p_i \mid a$. As the p_i are distinct primes, we conclude $q \mid a$ and hence $a + n\mathbb{Z} \in q\mathbb{Z}/n\mathbb{Z}$. Altogether we have the equality $\mathrm{JAC}(\mathbb{Z}_n) = q\mathbb{Z}/n\mathbb{Z}$.

Proof of (7.29):

(i) If $a \mid c \in \mathrm{cont}(f)$ then $a \mid c \mid f[\alpha]$ for any $\alpha \in \mathbb{N}^{\oplus I}$ say $f[\alpha] = a \cdot h[\alpha]$. Thereby $f = ah$ where $h \in A$ such that $a \mid f$ in A is granted. If conversely $a \mid h$ in A then $f = ah$ for some $h \in A$. But this is $f[\alpha] = a \cdot h[\alpha]$ such that $a \mid f[\alpha]$ for any $\alpha \in \mathbb{N}^{\oplus I}$. As c is a *greatest* common divisor of the $f[\alpha]$ this implies $a \mid c$.

(ii) If $c \in \mathrm{cont}(f)$ then by (i) we have $c \mid f$ such that $f = cf_1$ for some $f_1 \in A$. Take $b \in \mathrm{cont}(f_1)$, then $b \mid f_1$ such that $f_1 = bh$ for some $h \in A$. Hence $f = cbh$ which means $cb \mid f$. By (i) again this means $cb \mid c$ such that $b \mid 1$. That is $b \in R^{ast}$ such that f_1 is primitive.

Conversely if $f = cf_1$ for some primitive f_1 we take $d \in \mathrm{cont}(f)$. By (i) $c \mid f$ implies $c \mid d$. Let's say $d = ac$ Then by (i) again $ac = d \mid f = cf_1$ implies $a \mid f_1$ such that by (i) once again we get $a \mid 1$, as f_1 is primitive. That is $a \in R^*$ and hence $c \approx d \in \mathrm{cont}(f)$ which is $c \in \mathrm{cont}(f)$.

(iii) As $u \in B$ any coefficient $u[\alpha]$ is of the form $u[\alpha] = a[\alpha]/b[\alpha] \in E$, for some $a[\alpha]$ and $0 \neq b[\alpha] \in R$. As $u \neq 0$ there is some α with $u[\alpha] \neq 0$ and therefore we may take

$$b \;:=\; \mathrm{lcm}\Big(\Big\{ b[\alpha] \mid \alpha \in \mathbb{N}^{\oplus I}, u[\alpha] \neq 0 \Big\} \Big)$$

Note that we thereby take the least common multiple of a finite set and as R is an integral domain this implies $b \neq 0$ according to (2.57.(iii)). Then $(bu)[\alpha] = bu[\alpha] \in R$ for any $\alpha \in \mathbb{N}^{\oplus I}$ such that

$bu \in A$. Now let $a \in \mathrm{cont}(bu)$ and write $bu = au_1$ for some primitive $u_1 \in A$ using (ii). As $bu \neq 0$ it is clear, that $a \neq 0$, as well. Then we compute

$$bu \;=\; au \quad\Longrightarrow\quad u \;=\; \frac{a}{b}u_1$$

(iv) Let us first prove that the set $U \subseteq A$ of primitive polynomials is multiplicatively closed: As $\mathbf{1} \in A$ is a polynomial with $1 \in \mathrm{cont}(\mathbf{1})$ we have $1 \in U$. Now consider some $f, g \in U$ and let $c \in \mathrm{cont}(fg)$. If we had $c \notin R^*$ then [by prime decomposition of c] there would be some prime $p \in R$ such that $p \mid c$. By (i) this is $p \mid fg$ in A and by (7.27.(iii)) p is prime in A as well. W.l.o.g. we may take $p \mid g$ and if $d \in \mathrm{cont}(g)$ then this means $p \mid d$ according to (i). But g is primitive and hence $d \in R^*$ would imply $p \in R^*$ in contradiction to p being prime. This contradiction can only be avoided, if $c \in R^*$ and hence $1 \in \mathrm{cont}(fg)$. That is $fg \in U$ is primitive again.

By (ii) we may write $f = cf_1$ and $g = dg_1$ for some primitive f_1 and $g_1 \in A$. Then $fg = cd(f_1g_1)$ and as we have just seen f_1g_1 is primitive again. In particular we have $cd \in \mathrm{cont}(fg)$ according to (ii).

(v) Let us begin with the case in which $\star$ abbreviates *primitive*: Then we pick up primitive polynomials f and $g \in R[t]$ such that $u = \frac{a}{b}f$ and $v = \frac{c}{d}g$ according to (iii). In particular $bduv = acfg$. But as the content is multiplicative, we hence find

$$bd\,\mathrm{cont}(uv) \;=\; \mathrm{cont}(bduv) \;=\; \mathrm{cont}(acfg) \;=\; ac\,\mathrm{cont}(fg)$$

But by assumption uv is primitive and hence $1 \in \mathrm{cont}(uv)$. Also f and g are primitive and hence fg is primitive, due to (iv). That is $1 \in \mathrm{cont}(fg)$, as well and hence $bdR^* = acR^*$. That is we have $bd = \alpha ac$ for some $\alpha \in R^*$. Now let $u_1 := \alpha^{-1}f \in R[t]$ and $v_1 := g \in R[t]$, then we get $\frac{\alpha a}{b}u_1 = \frac{a}{b}f = u$, keep $\frac{c}{d}v_1 = \frac{c}{d}g = v$ and thereby also

$$uv \;=\; \frac{\alpha a}{b}u_1\frac{c}{d}v_1 \;=\; \frac{\alpha ac}{bd}u_1v_1 \;=\; \frac{\alpha ac}{\alpha ac}u_1v_1 \;=\; u_1v_1$$

That is we have found the properties (2) and (3) but property (1) also is clear, as from $u_1 = \alpha^{-1}f$ for some $\alpha \in R^*$ we get $1 \in \mathrm{cont}(f) = \mathrm{cont}(u_1)$. That is we have proved the statement for primitive polynomials.

Let us continue with the case in which $\star$ abbreviates the word *monic*: In particular the monic polynomial uv is primitive and hence we may use the case above, to find primitive polynomials $f, g \in R[t]$, such that $uv = fg$ and $u = \frac{a}{b}f$ and $v = \frac{c}{d}g$ again. But uv even is monic and R is an UFD (in particular an integral domain). Hence we may compare leading coefficients and find $1 = \mathrm{lc}(uv) = \mathrm{lc}(fg) = \mathrm{lc}(f)\mathrm{lc}(g)$, according to (7.18). That is $\alpha := \mathrm{lc}(f) \in R^*$ and also $\mathrm{lc}(g) = \alpha^{-1}$. Now define $u_1 := \alpha^{-1}f$ and $v_1 := \alpha g$, then clearly $u_1, v_1 \in R[t]$ are monic. We also get $u_1v_1 = \alpha^{-1}f\alpha g = fg = uv$ and $u = \frac{a}{b}f = \frac{\alpha a}{b}u_1$ and $v = \frac{c}{d}g = \frac{c}{d}\alpha^{-1}v_1 = \frac{c}{\alpha d}v_1$. That is we have properties (1), (2) and (3) in the monic case, as well.

(vi) The direction " $\Longrightarrow$ " is trivial: If $p \mid f$ in A then there is some $q \in A$ with $pq = f$. As $q \in A \subseteq B$ this is $p \mid f$ in B, as well. Conversely suppose $p \mid f$ in B, that is $pq = f$ for some $q \in B$. If $f = 0$ then $p \mid f = 0$ in A is granted by $q = 0$. Hence we only need to concern ourselves with $f \neq 0$.

In this case we also have $h \neq 0$ and using (iii) we may write $q = (c/b)q_1$ for some $c/b \neq 0$ and some primitive $q_1 \in A$. Now compute

$$bf \;=\; bpq \;=\; p(bq) \;=\; p(cq_1) \;=\; cpq_1$$

Let $b = \beta p_1 \dots p_k$ be a prime decomposition of b then for any $i \in 1 \dots k$ we have $p_i \mid b \mid bf = cpq_1$. And as $p_i \in R$ is prime, so is $p_i \in A$ due to (7.27.(iii)). This yields $p_i \mid c$ or $p_i \mid p$ or $p_i \mid q_1$. But both p and $q_1 \in A$ are primitive, so this only leaves $p_i \mid c$ by (i). And as this is true for any $i \in 1 \dots k$ we find $b \mid c$, say $ab = c$. Then we continue

$$bf \;=\; cpq_1 \;=\; abpq_1 \quad\Longrightarrow\quad f \;=\; apq_1$$

and thereby find, that truly $p \mid f$ in A. Let us summarize: We started with $f = pq$ for some $q \in B$, where $q = (c/b)q_1$. It turned out that $c/b = a \in R$ such that $f = pq$ with $q \in A$ already.

(vii) Let us first prove the claim in case $\star =$ *irreducible*: Suppose p is irreducible, as an element of A and consider $p = uv$ for some $u, v \in B$. By (iii) above there is some $0 \neq b/c \in E$ and some primitive $v_1 \in A$ such that $v = (c/b)v_1$ equivalently $bv = c = v_1$. Then

$$p \;=\; uv \;=\; \big(b^{-1}u\big)\big(bv\big) \;=\; \big(b^{-1}u\big)\big(cv_1\big) \;=\; \big(cb^{-1}u\big)v_1$$

Hence $v_1 \mid p$ in B and by (vi) that is $v_1 \mid p$ in A. That is we have $v_1 h = p$ for some $h \in A$. As p was assumed to be irreducible in A this implies v_1 or $h \in A^* = R^*$. Recall that $v = cb^{-1}v_1$ and $v_1 h = p = uv = ucb^{-1}v_1$. Then $h = cb^{-1}u$ and hence $u = bc^{-1}h$. If $v_1 \in R^*$ then $v = cb^{-1}v_1 \in E^* = B^*$ and if $h \in R^*$ then $u = bc^{-1}h \in E^* = B^*$. Therefore p is irreducible in B. [Note that we did not require the primivitity of p for this direction].

Conversely suppose p is irreducible, as an element of B and consider $p = fg$ for some $f, g \in A$. In particular f or $g \in B^* = E^*$. W.l.o.g. let us assume $f \in E^*$. That is $f = f[0] \neq 0$. If now $c \in \mathrm{cont}(f)$ and $d \in \mathrm{cont}(g)$, then by (iv) we have $cd \in \mathrm{cont}(fg) = \mathrm{cont}(p)$. But p was assumed to be primitive and hence $\mathrm{cont}(p) = R^*$ such that $c \in R^*$. But as $f = f[0]$ we have $f[0] \in \mathrm{cont}(f) = cR^* = R^*$ and therefore $f \in R^* = A^*$. And this is the irreducibility of p in A.

Now we prove the claim in case $\star =$ *prime*: Suppose p is prime, as an element of B. As we want to prove that p is prime in A we consider some $f, g \in A$ such that $p \mid fg$ in A. In particular $p \mid fg$ in B and hence $p \mid f$ or $p \mid g$ in B. But by (vi) this is $p \mid f$ or $p \mid g$ in A and this is the prime property of p in A.

Conversely suppose p is prime as an element of A and remember $p \notin R$. We need to show that p is prime in B, that is we consider $u, v \in B$ such that $p \mid uv$ in B. By (iii) there are some $a, b \in R$ such that au and $bv \in A$. And $p \mid uv$ implies $p \mid (au)(bv)$ in B, as well. But as p is primitive (i) implies $p \mid (au)(bv)$ in A from which we get $p \mid au$ or $p \mid bv$ in A, as p was assumed to be prime in A. Once again this implies $p \mid a$ or $p \mid u$ or $p \mid b$ or $p \mid v$ in A. But as $a, b \in R$ and $p \notin R$ the possibilities $p \mid a$ and $p \mid b$ are absurd, so we are left with $p \mid u$ or $p \mid v$ in A. Trivially this implies $p \mid u$ or $p \mid v$ in B, such that p is prime in B.

(viii) Let us fist prove the implication A is an UFD $\Longrightarrow$ R is an UFD. As R is a sub-ring of A and A

is an UFD, R is an integral domain. Now consider any $0 \neq a \in R$, by assumption a has a prime decomposition $a = \alpha p_1 \dots p_k$ in A, that is $\alpha \in A^* = R^*$ and $p_i \in A$ are prime. As $a \in R$ we have $p_i \in R$ by (7.22). As p_i is prime in A so it is in R, by (7.27.(iii)). Thus we already have a prime decomposition $a = \alpha p_1 \dots p_k$ of a. And as $a \neq 0$ was arbitrary this means that R is an UFD.

The proof of the converse implication R is an UFD $\implies$ A is an UFD will be conducted in three steps: In a first step let us assume $\#I = 1$, that is $A = R[t]$ is the polynomial ring in one variable. By assumption R is an UFD, then we need to show that $A = R[t]$ is an UFD, as well. We already know that A is an integral domain, by (7.12.(vii)). Now consider any $0 \neq f \in A$, if $\deg(f) = 0$ then $f \in R$ and as R was assumed to be an UFD we find a prime decomposition $f = \alpha p_1 \dots p_k$ in R. As any $p_i \in R$ is prime in R, it also is prime in A, once more. Also $\alpha \in R^* = A^*$ such that $f = \alpha p_1 \dots p_k$ also is a prime decomposition of f in A. If $\deg(f) \geq 1$, then we note that $B = E[t]$ is a PID and in particular an UFD by (2.71.(iii)) and (2.79.(ii)) respectively. Therefore f has a prime decomposition $f = \alpha v_1 \dots v_k$ in B. That is $\alpha \in B^* = E^*$ and $v_i \in B$ are prime. In particular we have $v_i \notin E$. By above there are some $0 \neq c_i/b_i \in E$ and primitive $p_i \in A$ such that $v_i = (c_i/b_i)p_i$. Note that $p_i \notin R$, as $v_i \notin E$. Now define $b := b_1 \dots b_k$ and $c := c_1 \dots c_k$ and $p := p_1 \dots p_k$ then we compute

$$bf \;=\; \alpha b \prod_{i=1}^{k} v_i \;=\; \alpha \prod_{i=1}^{k} (b_i v_i) \;=\; \alpha \prod_{i=1}^{k} (c_i p_i) \;=\; \alpha c p$$

As the $p_i \in A$ are primitive, so is p, due to (iv). And as $f = \alpha(c/b)p$ we have $p \mid f$ in B. But by (vi) this implies $p \mid f$ in A such that $ph = f$ for some $h \in A$. That is $ph = f = \alpha(c/b)p$ such that $h = \alpha(c/b) \in A \cap E^* = R \setminus \{0\}$. As R is an UFD h admits a prime decomposition in R. And by (7.27.(iii)) this also is a prime decomposition in A. Also $c_i p_i = b_i v_i$ implies $p_i = (b_i/c_i)v_i \approx v_i$ in B. As v_i is prime in B this implies that p_i is prime in B, as well. And by (vi) p_i is prime in A such that $p = p_1 \dots p_k$ is a prime decomposition of p. As both h and p have a prime decomposition, so does $f = ph$. And as f was arbitrary this shows, that A is an UFD.

If $\#I < \infty$, say $I = \{1, \dots, n\}$ then we can prove the equivalence of R and A being UFDs by induction on n: The case $n = 1$ has just been established and for the induction step we use the isomorphy (7.23.(iii))

$$R[t_1, \dots, t_n, t_{n+1}] \quad \cong_{\mathsf{a}} \; A[t_{n+1}]$$

where $A := R[t_1, \dots, t_n]$. By induction hypothesis R is an UFD if and only if A is such. And by the case $n = 1$ we know that A is an UFD if and only if $A[t_{n+1}]$ is such. Thus R is an UFD if and only if $A[t_{n+1}]$ and hence $R[t_1, \dots, t_n, t_{n+1}]$ is such. Thus the induction is complete.

For general I we note that any $f \in A$ is contained in a polynomial ring with finitely many variables only. To be precise let

$$\Omega \;:=\; \Big\{ i \in I \mid \exists\, \alpha \in \mathbb{N}^{\oplus I} \,:\, f[\alpha] \neq 0 \text{ and } \alpha_i \neq 0 \Big\}$$

then we have $f \in R[t_i \mid i \in \Omega]$ and $\Omega \subseteq I$ is finite since there are finitely many α with $f[\alpha] \neq 0$ only and all of these have $\alpha_i \neq 0$ for finitely many $i \in I$ only. Thus as R is an UFD and Ω is finite $S := R[t_i \mid i \in \Omega]$ is an UFD, as well. Thus any $0 \neq f \in S$ has a prime decomposition $f = \alpha p_1 \dots p_k$ in S. That is $\alpha \in S^* = R^*$ and the $p_i \in S$ are prime. As $A = R[t_i \mid i \in I] \;\cong_{\mathsf{a}}\; S[t_i \mid i \in I \setminus \Omega]$

we find by (7.27.(iii)) that the p_i are prime in A, as well. Thus $f = \alpha p_1 \dots p_k$ also is a prime decomposition of f in A. And as f was arbitrary this means that A is an UFD.

□

Proof of (7.30):

(i) We have to verify that for any two Laurent series $f, g \in L$ and any $\gamma \in \mathbb{Z}^n$ the set $I := \{ (\alpha, \beta) \mid \alpha + \beta = \gamma, f[\alpha] \neq 0, g[\beta] \neq 0 \}$ of indexes is finite. To show this let us denote $[\alpha] := \min\{ \alpha_i \mid i \in 1 \dots n \}$. As $f \in L$ by definition there is some $k \in \mathbb{Z}$ such that $f[\alpha] \neq 0$ implies $[\alpha] \geq k$ and likewise $g[\beta] \neq 0$ implies $[\beta] \geq \ell$ for some $\ell \in \mathbb{Z}$. Then it is clear, that $I \subseteq \{ (\alpha, \beta) \mid \alpha + \beta = \gamma, k \leq [\alpha], \ell \leq [\beta] \}$. And clearly we have $[\alpha + \beta] \geq [\alpha] + [\beta]$ such that $[\gamma] = [\alpha + \beta] \geq [\alpha] + [\beta] \geq [\alpha] + \ell$ from which we get $[\alpha] \leq [\gamma] - \ell$. Inserting $\beta = \gamma - \alpha$ and this inequality into I we finally get the upper bound $I \subseteq \{ (\alpha, \gamma - \alpha) \mid k \leq [\alpha] \leq [\gamma] - \ell \}$ and this finally is a finite set.

(ii) If $f \in L$ then by definition there is some $\ell \in \mathbb{Z}$ such that $f[\alpha] \neq 0$ implies $\alpha_i \geq \ell$ and hence (since $\omega_i \geq 0$ as well) we get $\omega_i \alpha_i \geq \omega_i \ell$. Altogether

$$|\alpha|_\omega \;=\; \sum_{i=1}^{n} \omega_i \alpha_i \;\geq\; \sum_{i=1}^{n} \omega_i \ell \;=\; |\omega| \cdot \ell$$

Hence the set $\{ |\alpha|_\omega \mid \alpha \in \mathbb{Z}^n,\ f[\alpha] \neq 0 \}$ is bounded from below, by $|\omega| \cdot \ell$ and therefore has a minimal element.

(iii) Let us define a partial order on $\mathbb{Z}^n$ by taking $\alpha \leq \beta$ if and only if $|\alpha|_\omega \geq |\beta|_\omega$. Then $\leq$ even is a positive order on $\mathbb{Z}^n$, as for any α, α' and $\beta \in \mathbb{Z}^n$ we get: $\alpha \leq \alpha'$ is $|\alpha|_\omega \geq |\alpha'|_\omega$ such that $|\alpha + \beta|_\omega = |\alpha|_\omega + |\beta|_\omega \geq |\alpha'|_\omega + |\beta|_\omega = |\alpha' + \beta|_\omega$ which again is $\alpha + \beta \leq \alpha' + \beta$. And also we find the equality

$$\begin{aligned} \operatorname{ord}_\omega(f) &= \min\{ |\alpha|_\omega \mid f[\alpha] \neq 0 \} \\ &= |\max\nolimits_{\leq} \{ \alpha \mid f[\alpha] \neq 0 \}|_\omega \;=\; |\deg(f)|_\omega \end{aligned}$$

And as $\mathbb{Z}^n$ is an integral monoid (it even is a group) we find the following inequality (with respect the positive order $\leq$ on $\mathbb{Z}^n$) according to (7.18)

$$\deg(f\,g) \;\leq\; \deg(f) + \deg(g)$$

And by definition of $\leq$ this is $|\deg(f\,g)|_\omega \geq |\deg(f) + \deg(g)|_\omega = |\deg(f)|_\omega + |\deg(f)|_\omega$ again. And from this the above equality implies $\operatorname{ord}_\omega(f\,g) \geq \operatorname{ord}_\omega(f) + \operatorname{ord}_\omega(g)$. If R is an integral domain (as $\mathbb{Z}^n$ being a group and hence integral, too) then (7.18) even yields an equality here. And for arbitrary R we already get

$$\deg(f+g) \;\leq\; \max\{ \deg(f), \deg(g) \}$$

with respect to the positive order $\leq$. But according to its definition this is $|\deg(f+g)|_\omega \geq \min\{ |\deg(f)|_\omega, |\deg(g)|_\omega \}$ again, such that we also get $\operatorname{ord}_\omega(f+g) \geq \min\{ \operatorname{ord}_\omega(f), \operatorname{ord}_\omega(g) \}$.

(iv) Clearly U is multiplicatively closed, as $(\mathbb{N}^n,+) \to (P,\cdot) : \alpha \mapsto t^\alpha$ is a monoid homomorphism, whose image is U precisely. As t^α has the inverse element $t^{-\alpha} \in L$ we also have $U \subseteq L^*$. Thus, regarding the embedding $\iota : P \to L : f \mapsto f$, we see that $\iota(U) \in L^*$. Hence the universal property of localization of rings (2.120) yields a well-defined homomorphism of rings $\Phi := \bar{\iota} : U^{-1}P \to L$ by taking $\Phi(f/t^\alpha) = f \cdot t^{-\alpha}$. It remains to show, that this homomorphism in fact is an isomorphism. For the injectivety let us take some f, $g \in P$ and α, $\beta \in \mathbb{N}^n$ such that $t^{-\alpha}f = t^{-\beta}g$. But multiplying this equality with $t^{0+\alpha+\beta}$ we get $t^0 t^\beta f = t^0 t^\alpha g$ such that truly $f/t^\alpha = g/t^\beta$. For the surjectivety we are given some $g \in L$ and need to find $f \in P$ and $\alpha \in \mathbb{N}^n$ such that $g = t^{-\alpha}f$. To do this we define $\alpha_i \in \mathbb{N}$ as follows: if $\mathrm{ord}_i(g) \geq 0$ take $\alpha_i := 0$ otherwise - if $\mathrm{ord}_i(g) < 0$ - take $\alpha_i := -\mathrm{ord}_i(g) > 0$. Then it is clear that $\alpha_i \geq 0$ and hence $\alpha \in \mathbb{N}^n$. Letting $f := t^\alpha g$ we get $\mathrm{ord}_i(f) \geq \mathrm{ord}_i(t^\alpha) + \mathrm{ord}_i(g) = \alpha_i + \mathrm{ord}_i(g)$. If $\mathrm{ord}_i(g) \geq 0$ then $\alpha_i = 0$ and hence $\mathrm{ord}_i(f) = \mathrm{ord}_i(g) \geq 0$. If conversely $\mathrm{ord}_i(g) < 0$, then $\alpha_i = -\mathrm{ord}_i(g)$ and hence $\mathrm{ord}_i(f) = 0$. In any case we have $\mathrm{ord}_i(f) \geq 0$ and hence $f \in P$. And by construction it is clear, that $g = t^{-\alpha}f$ establishing the surjectivety of Φ.

(v) If $f \in R[\![t]\!]$ is invertible, then there is some $g \in R[\![t]\!]$ such that $fg = 1$. In particular we get $1 = 1[0] = fg[0] = f[0] \cdot g[0]$ and hence $f[0] \in R$ is invertible, too. Conversely suppose are given som $f \in R[\![t]\!]$ such that $f[0] \in R^*$. Then we need to find some $g \in R[\![t]\!]$ such that $fg = 1$. To do this first recall the definition of fg:

$$\begin{aligned} fg &= \left(\sum_{i=0}^{\infty} f[i]t^i\right)\left(\sum_{j=0}^{\infty} g[j]t^j\right) \\ &= \sum_{k=0}^{\infty}\left(\sum_{i+j=k} f[i]\cdot g[j]\right)t^k \\ &= \sum_{k=0}^{\infty}\left(\sum_{j=0}^{k} f[k-j]\cdot g[j]\right)t^k \end{aligned}$$

Let us now construct g with $fg = 1$ by recursively defining its coefficients, starting with $g[0] := f[0]^{-1} \in R$. Suppose we already have $g[0],\ldots,g[k-1]$, then we take $g[k]$ to be

$$g[k] := -f[0]^{-1}\left(\sum_{j=1}^{k-1} f[k-j]g[j]\right)$$

We will now prove $fg = 1$: First of all $fg[0] = f[0]\cdot g[0] = f[0]\cdot f[0]^{-1} = 1$ is clear and for $k \geq 1$ we also find $fg[k] = 0$ by construction

$$fg[k] = \sum_{j=0}^{k} f[k-j]\cdot g[j] = \sum_{j=0}^{k-1} f[k-j]\cdot g[j] + f[0]\cdot g[k] = 0$$

(vi) Clearly $t^{-\mathrm{ord}(g)}f \in L$ and according to (v) we also find that $t^{-\mathrm{ord}(g)}g \in P^* \subseteq L^*$ is invertible. Hence the expression

$$\Phi(f/g) := t^{-\mathrm{ord}(g)}f \cdot (t^{-\mathrm{ord}(g)}g)^{-1}$$

is well-defined. Next we will prove that the homomorphism Φ is well-defined, as well. To do this

consider f, g, h and $k \in P$ with $g, k \neq 0$ such that $f/g = h/k$. Let us also abbreviate $u := t^{-\mathrm{ord}(g)}g$ and $v := t^{-\mathrm{ord}(k)}k$, then $f/g = h/k$ means $fk = gh$ since P is an integral domain. And multiplying this equation with $t^{-\mathrm{ord}(gk)}$ we get

$$t^{-\mathrm{ord}(g)}fv \;=\; t^{-\mathrm{ord}(g)}ft^{-\mathrm{ord}(k)}k \;=\; t^{-\mathrm{ord}(g)}gt^{-\mathrm{ord}(k)}h \;=\; t^{-\mathrm{ord}(k)}hu$$

But multiplying this equation with $u^{-1}v^{-1}$ again, we find $\Phi(f/g) = t^{-\mathrm{ord}(g)}fu^{-1} = t^{-\mathrm{ord}(k)}hv^{-1} = \Phi(h/k)$ which had to be shown. As all these equations have been equivalent this already establishes the injectivety of Φ. So let us now turn our attention to the homomorphism properties of Φ:

$$\begin{aligned}
\Phi\left(\frac{f}{g}\cdot\frac{h}{k}\right) &= \Phi\left(\frac{fh}{gk}\right) \;=\; t^{-\mathrm{ord}(gk)}fh\left(t^{-\mathrm{ord}(gk)}gk\right)^{-1} \\
&= t^{-\mathrm{ord}(g)}t^{-\mathrm{ord}(k)}fh\left(t^{-\mathrm{ord}(g)}t^{-\mathrm{ord}(k)}gk\right)^{-1} \\
&= t^{-\mathrm{ord}(g)}ft^{-\mathrm{ord}(k)}h\left(t^{-\mathrm{ord}(g)}g\right)^{-1}\left(t^{-\mathrm{ord}(k)}k\right)^{-1} \\
&= \Phi\left(\frac{f}{g}\right)\Phi\left(\frac{h}{k}\right) \\
\Phi\left(\frac{f}{g}+\frac{h}{k}\right) &= \Phi\left(\frac{fk+gh}{gk}\right) \;=\; t^{-\mathrm{ord}(gk)}(fk+gh)\left(t^{-\mathrm{ord}(gk)}gk\right)^{-1} \\
&= \left(t^{-\mathrm{ord}(g)}fv + t^{-\mathrm{ord}(k)}hu\right)(uv)^{-1} \\
&= t^{-\mathrm{ord}(g)}fu^{-1} + t^{-\mathrm{ord}(k)}hv^{-1} \;=\; \Phi\left(\frac{f}{g}\right)+\Phi\left(\frac{h}{k}\right)
\end{aligned}$$

It remains to prove the surjectivety if Φ: To do this consider any $\ell \in L$. If $\mathrm{ord}(\ell) \geq 0$, then $\ell \in P$ already and we take $r := 0$. Conversely, if $\mathrm{ord}(\ell) < 0$ then we take $r := -\mathrm{ord}(\ell) > 0$. Thus we always have $r \geq 0$ and hence $t^r \in P$. We also get $\mathrm{ord}(t^r\ell) = r + \mathrm{ord}(\ell) \geq 0$ such that $t^r\ell \in P$. Therefore we can compute

$$\Phi\left(\frac{t^r\ell}{t^r}\right) = t^{-\mathrm{ord}(t^r)}t^r\ell\left(t^{-\mathrm{ord}(t^r)}t^r\right)^{-1} = t^{-r}t^r\ell(t^{-r}t^r)^{-1} = \ell 1^{-1} = \ell$$

□

Proof of (7.70):

(i) By the product rule of derivations we find $d(1_A) = d_1(1_A \cdot 1_A) = d(1_A)\cdot 1_A + 1_A \cdot d(1_A) = d(1_A) + d(1_A)$. By subtracting $d(1_A)$ once, we obtain $0_A = d(1_A)$ from this. And as d also is R-linear $d(a1_A) = ad(1_A) = a0_A = 0_A$ for any $a \in R$, as well.

(ii) Let us prove the general product rule by induction on n. For $n = 1$ the identity is obvious, we only have $d(f_1)$ on both sides. For the induction step $n \mapsto n+1$ let us abbreviate $f := f_1 \cdot \ldots \cdot f_n$, then we use the product rule and induction hypothesis on the following term

$$d\big(f_1 \cdot \ldots \cdot f_{n+1}\big) \;=\; d\big(f \cdot f_{n+1}\big) \;=\; d(f)\cdot f_{n+1} + f \cdot d\big(f_{n+1}\big)$$

$$
\begin{aligned}
&= \left(\sum_{i=1}^{n} f_1 \cdot \ldots \cdot f_{i-1} \cdot d(f_i) \cdot f_{i+1} \cdot \ldots \cdot f_n\right) \cdot f_{n+1} + (f_1 \cdot \ldots \cdot f_n) \cdot d\big(f_{n+1}\big) \\
&= \sum_{i=1}^{n+1} f_1 \cdot \ldots \cdot f_{i-1} \cdot d(f_i) \cdot f_{i+1} \cdot \ldots \cdot f_{n+1}
\end{aligned}
$$

(iii) The first identity is clear by (ii): As A is commutative any of the n summands is of the form $d(f) \cdot f^{n-1}$ and as we have n summands this turns into $nd(f) \cdot f^{n-1}$. The second identity is clear for $m = 0$: $d^m(f \cdot g) = \mathbb{1}(f \cdot g) = f \cdot g$, same as $d^0(f) \cdot d^0(g) = f \cdot g$. For $m \geq 1$ we use induction on m. But this is a straightforward computation, basically, that uses the binomial recursion formula

$$
\begin{aligned}
d^{m+1}(f \cdot g) &= d\Big(d^m(f \cdot g)\Big) = d\left(\sum_{k=0}^{m} \binom{m}{k} d^k(f) \cdot d^{m-k}(g)\right) \\
&= \sum_{k=0}^{m} \binom{m}{k} d\big(d^k(f) \cdot d^{m-k}(g)\big) \\
&= \sum_{k=0}^{m} \binom{m}{k} \big(d^{k+1}(f) \cdot d^{m-k}(g) + d^k(f) \cdot d^{m-k+1}(g)\big) \\
&= \sum_{k=1}^{m} \binom{m}{k-1} d^k(f) \cdot d^{m-(k-1)}(g) + \sum_{k=0}^{m} \binom{m}{k} d^k(f) \cdot d^{m-k+1}(g) \\
&= d^{m+1}(f) \cdot g + \sum_{k=1}^{m} \left(\binom{m}{k-1} + \binom{m}{k}\right) d^k(f) \cdot d^{m+1-k}(g) + f \cdot d^{m+1}(g) \\
&= d^{m+1}(f) \cdot g + \sum_{k=1}^{m} \binom{m+1}{k} d^k(f) \cdot d^{m+1-k}(g) + f \cdot d^{m+1}(g) \\
&= \sum_{k=0}^{m+1} \binom{m+1}{k} d^k(f) \cdot d^{m+1-k)}(g)
\end{aligned}
$$

(iv) Let us first check the well-definedness of $U^{-1}d$: That is we start with any $f/u = g/v \in U^{-1}A$. That is $wvf = wug$ for some $w \in U$. This is $w(vf - ug) = 0$ and as U does not contain any zero-divisors, we get $vf - ug = 0$ which is $vf = ug$. Using this we have to show

$$
\frac{d(f) \cdot u - f \cdot d(u)}{u^2} = \frac{d(g) \cdot v - g \cdot d(v)}{v^2}
$$

Again we can omit the $w \in U$, as U does not contain zero-divisors such that this equation means $v^2(d(f) \cdot u - f \cdot d(u)) = u^2(d(g) \cdot v - g \cdot d(v))$. Rearranging terms, this equation is equivalent, to

$$
uv^2 d(f) + u^2 g d(v) = u^2 v d(g) + v^2 f d(u)
$$

In this equation we replace $u^2 g = u(ug)$ by $u(vf) = uvf$ and likewise we replace $v^2 f = v(vf)$ by $v(ug) = uvg$. Doing this we can factor out uv on both sides, to end up with the following equation

$$
uv\big(vd(f) + fd(v)\big) = uv\big(ud(g) + gd(u)\big)
$$

Yet $vf = ug$ also implies that $d(vf) = vd(f) + fd(v)$ equals $d(ug) = ud(g) + gd(u)$ such that the last equality holds true. Altogether we get the identity needed and thereby the well-definedness

of $U^{-1}d$. And as $d(1_A) = 0_A$ it is straightforward to see, that

$$U^{-1}d\left(\frac{f}{1}\right) \;=\; \frac{d(f)\cdot 1 - f\cdot d(1)}{1} \;=\; \frac{d(f)}{1}$$

So it remains to verify, that $U^{-1}d$ truly is a derivation on $U^{-1}A$. We commence by proving, the R-linearity, followed by the product rule. Consider any $a \in R$, f and $g \in A$ and u, $v \in U$, then we compute

$$\begin{aligned}
U^{-1}d\left(a\frac{f}{u}\right) &= U^{-1}d\left(\frac{af}{u}\right) = \frac{d(af)\cdot u - (af)\cdot d(u)}{u^2} \\
&= \frac{a\big(d(f)\cdot u - f\cdot d(u)\big)}{u^2} = a\frac{d(f)\cdot u - f\cdot d(u)}{u^2} \\
U^{-1}d\left(\frac{f}{u}+\frac{g}{v}\right) &= U^{-1}d\left(\frac{fv+gu}{uv}\right) \\
&= \frac{d(fv+gu)\cdot uv - (fv+gu)\cdot d(uv)}{u^2v^2}
\end{aligned}$$

The last term needs to be decomposed in parts: $d(fv+gu) = d(fv)+d(gu)$ as d is additive and using the product rule, this turns into $d(f)v + fd(v) + d(g)u + gd(u)$. Multiplying this by uv yields $uv^2d(f) + fuvd(v) + u^2vd(g) + guvd(u)$. Now for the second part: $d(uv) = d(u)v + ud(v)$. Multiplying this by fv yields $fv^2d(u) + fuvd(v)$. Likewise multiplication of $d(uv)$ by gu yields $guvd(u) + gu^2d(v)$. We see, that both $fuvd(v)$ and $guvd(u)$ occurs in the first and second parts and hence cancels each other, it only remains

$$\begin{aligned}
U^{-1}d\left(\frac{f}{u}+\frac{g}{v}\right) &= \frac{uv^2d(f) + u^2vd(g) - fv^2d(u) - gu^2d(v)}{u^2v^2} \\
&= \frac{uv^2d(f) - fv^2d(u)}{u^2v^2} + \frac{u^2vd(g) - gu^2d(v}{u^2v^2} \\
&= \frac{ud(f) - fd(u)}{u^2} + \frac{vd(g) - gd(v)}{v^2} \\
&= U^{-1}d\left(\frac{f}{u}\right) + U^{-1}d\left(\frac{g}{v}\right) \\
U^{-1}d\left(\frac{f}{u}\cdot\frac{g}{v}\right) &= U^{-1}d\left(\frac{fg}{uv}\right) = \frac{d(fg)\cdot uv - (fg)\cdot d(uv)}{u^2v^2} \\
&= \frac{guvd(f) + fuvd(g) - fgvd(u) - fgud(v)}{u^2v^2} \\
&= \frac{guvd(f) - fgvd(u)}{u^2v^2} + \frac{fuvd(g) - fgud(v)}{u^2v^2} \\
&= \frac{ud(f) - fd(u)}{u^2}\cdot\frac{gv}{v^2} + \frac{fu}{u^2}\cdot\frac{vd(g) - gd(v)}{v^2} \\
&= U^{-1}d\left(\frac{f}{u}\right)\cdot\frac{g}{v} + \frac{f}{u}\cdot U^{-1}d\left(\frac{g}{v}\right)
\end{aligned}$$

(v) The map $d \mapsto U^{-1}d$ is well-defined, according to (iv). It also is infective: Consider any two derivations d_1 and $d_2 \in \mathrm{der}(A)$ such that $U^{-1}d_1 = U^{-1}d_2$, then for any $f \in A$ we get

$$\frac{d_1(f)}{1} \;=\; U^{-1}d_1\left(\frac{f}{1}\right) \;=\; U^{-1}d_2\left(\frac{f}{1}\right) \;=\; \frac{d_2(f)}{1}$$

That is there is some $w \in U$ such that $wd_1(f) = wd_2(f)$, but as U does not contain any zero-divisors this is $d_1(f) = d_2(f)$ for any $f \in A$ and hence $d_1 = d_2$. The R-linearity of $d \mapsto U^{-1}d$ can be proved in a straightforward computation

$$\begin{aligned}
U^{-1}(ad)\left(\frac{f}{u}\right) &= \frac{(ad)(f)\cdot u - f\cdot(ad)(u)}{u^2} = \frac{ad(f)\cdot u - f\cdot ad(u)}{u^2} \\
&= a\frac{d(f)\cdot u - f\cdot d(u)}{u^2} = aU^{-1}d\left(\frac{f}{u}\right) \\
U^{-1}(d_1+d_2)\left(\frac{f}{u}\right) &= \frac{(d_1+d_2)(f)\cdot u - f\cdot(d_1+d_2)(u)}{u^2} \\
&= \frac{d_1(f)\cdot u + d_2(f)\cdot u - f\cdot d_1(u) - f\cdot d_2(u)}{u^2} \\
&= \frac{d_1(f)\cdot u - f\cdot d_1(u)}{u^2} + \frac{d_2(f)\cdot u - f\cdot d_2(u)}{u^2} \\
&= U^{-1}d_1\left(\frac{f}{u}\right) + U^{-1}d_2\left(\frac{f}{u}\right)
\end{aligned}$$

If $d \in \mathrm{der}(A)$, then $U^{-1}d(f/1) = d(f)/1$, as we have seen in (iv). Conversely, if $D \in \mathrm{der}(U^{-1}A)$ safisfies $D(f/1) = f'/1$ for some $f' \in A$, then $d : f \mapsto f'$ is a derivation on A. The R-linearity is clear and the product-rule follows from

$$\frac{(fg)'}{1} = D\left(\frac{fg}{1}\right) = D\left(\frac{f}{1}\right)\cdot\frac{g}{1} + \frac{f}{1}\cdot D\left(\frac{g}{1}\right) = \frac{f'\cdot g + f\cdot g'}{1}$$

By construction we have $D(f/1) = d(f)/1$, it remains to verify $D = U^{-1}d$: As D is a derivation we have $D(1/1) = 0$, but $u/u = 1/1$ such that $0 = D(u/u) = D(u/1)\cdot 1/u + u/1\cdot D(1/u)$ and this turns into $D(1/u) = -D(u/1)\cdot 1/u^2 = -d(u)/u^2$. Using this, we compute

$$\begin{aligned}
D\left(\frac{f}{u}\right) &= D\left(\frac{f}{1}\cdot\frac{1}{u}\right) = \frac{d(f)}{1}\cdot\frac{1}{u} + \frac{f}{1}\cdot D\left(\frac{1}{u}\right) \\
&= \frac{d(f)\cdot u}{u^2} - \frac{f}{1}\cdot\frac{d(u)}{u^2} = \frac{d(f)\cdot u - f\cdot d(u)}{u^2} = U^{-1}d\left(\frac{f}{u}\right)
\end{aligned}$$

□

Proof of (7.71):
First note, that by definition we have $(t^k)' = kx^{k-1}$ for $k \geq 1$ and $(t^k)' = 0$ for $k = 0$. By abuse of notation we can write this, as $(t^k)' = kt^{-1}$ even for $k = 0$, as $k = 0$ eliminates the term, even though t^{-1} is not a well defined element of $R[t]$. Then f' is defined by linear expansion of $d : t^k \mapsto kt^{k-1}$ from the R-basis $\left\{ t^k \mid k \in \mathbb{N} \right\}$ of $R[t]$. In particular $d : f \mapsto f'$ is R-linear. It remains to verify the product rule for any polynomials $f, g \in R[t]$:

$$(f\cdot g)' = \left(\sum_{k=0}^{\infty}\left(\sum_{i+j=k} f[i]g[j]\right)t^k\right)' = \sum_{k=1}^{\infty}\left(\sum_{i+j=k} f[i]g[j]\right)kt^{k-1}$$

Note that we may formally extend the sum to $k = 0$, as the 0-th summand is 0. Also note that we have the identity $kt^{k-1} = (i+j)t^{i+j-1} = it^{i+j-1} + jt^{i+j-1} = it^{i-1}\cdot t^j + t^i jt^{j-1} = (t^i)'\cdot t^j + t^i\cdot(t^j)'$ such that

we may continue our computation with the expression

$$\begin{aligned}
(f\cdot g)' &= \sum_{k=1}^{\infty}\left(\sum_{i+j=k} f[i]g[j]\right)\left((t^i)'\cdot t^j + t^i\cdot(t^j)'\right)\\
&= \sum_{k=0}^{\infty}\left(\sum_{i+j=k} f[i]g[j]\left((t^i)'\cdot t^j + t^i\cdot(t^j)'\right)\right)\\
&= \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} f[i]g[j]\left((t^i)'\cdot t^j + t^i\cdot(t^j)'\right)\\
&= \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} f[i](t^i)'g[j]t^j + \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} f[i]t^i g[j](t^j)'\\
&= \left(\sum_{i=0}^{\infty} f[i](t^i)'\right)\cdot\left(\sum_{j=0}^{\infty} g[j]t^j\right) + \left(\sum_{i=0}^{\infty} f[i]t^i\right)\cdot\left(\sum_{j=0}^{\infty} g[j](t^j)'\right)\\
&= \left(\sum_{i=0}^{\infty} f[i]t^i\right)'\cdot\left(\sum_{j=0}^{\infty} g[j]t^j\right) + \left(\sum_{i=0}^{\infty} f[i]t^i\right)\cdot\left(\sum_{j=0}^{\infty} g[j]t^j\right)'\\
&= f'\cdot g + f\cdot g'
\end{aligned}$$

□

Proof of (7.73):

(i) As the partial derivatives are defined by linear expansion, it suffices to check the commutativity on the basis elements t^α for some $\alpha = (\alpha_1,\ldots,\alpha_n)\in\mathbb{N}$. If $i=j$, then $\partial_i\partial_j = \partial_j\partial_i$ is trivial. For $i\neq j$ we distinguish two cases: (1) If $\alpha_i = 0$ or $\alpha_j = 0$ then $\partial_i t^\alpha = 0$ or $\partial_j t^\alpha = 0$. In both cases we get $\partial_i\partial_j t^\alpha = 0$ and likewise $\partial_j\partial_i t^\alpha = 0$ respectively. (2) If $\alpha_i \geq 1$ and $\alpha_j \geq 1$ then it is easy to see, that $\partial_i\partial_j t^\alpha = \partial_i(\alpha_j t^{\alpha-\delta_j}) = \alpha_j\partial_i(t^{\alpha-\delta_j}) = \alpha_j\alpha_i t^{\alpha-\delta_j-\delta_j}$ and likewise $\partial_j\partial_i t^\alpha = \alpha_i\alpha_j t^{\alpha-\delta_i-\delta_j}$. In both cases (1) and (2) we see that $\partial_i\partial_j t^\alpha$ and $\partial_j\partial_i t^\alpha$ are equal and hence this is also true for any polynomial $f\in R[t_1,\ldots,t_n]$

$$\partial_i\partial_j f \;=\; \sum_{\alpha\in\mathbb{N}^n} f[\alpha]\,\partial_i\partial_j t^\alpha \;=\; \sum_{\alpha\in\mathbb{N}^n} f[\alpha]\,\partial_j\partial_i t^\alpha \;=\; \partial_j\partial_i f$$

(ii) Let us first consider the case $n=1$: For any $i,j\in\mathbb{N}$ we will prove $\partial^i t^j = (j!/(j-i)!)t^{j-i}$ by induction on i: As $\partial^0 = \mathbb{1}$ the statement is true for $i=0$. And for $i=1$ we have $\partial^i = \partial$ such that $\partial t^j = jt^{j-1} = (j!/(j-1)!)t^{j-i}$ [and $\partial t^j = 0$ for $j=0$] is just the definition of the formal derivative ∂. Now for the induction step $i-1\mapsto i$ we use this definition once more

$$\partial^i t^j \;=\; \partial\partial^{i-1}t^j \;=\; \partial\left(\frac{j!}{(j-i+1)!}t^{j-i+1}\right) \;=\; \frac{j!}{(j-i+1)!}(j-i+1)t^{j-i+1-1} \;=\; \frac{j!}{(j-i)!}t^{j-i}$$

in case $i\leq j$. If $i=j+1$ then we note that $\partial^j t^j = j!$ is of degree zero, such that $\partial^i t^j = \partial\partial^j t^j = 0$. And finally for $i>j+1$ we already have $\partial^{i-1}t^j = 0$ already, such that $\partial^i t^j = 0$ stays true. Altogether we have proved the claim in case $n=1$.

Let us now use induction on the number n of variables of the polynomial ring. The case $n=1$ has already been dealt with, so we commence with the induction step $n\mapsto n+1$: That is we have to take a look at $\alpha' = (\alpha,\alpha_{n+1})$ where $\alpha = (\alpha_1,\ldots,\alpha_n)$ and likewise the same for $\beta' = (\beta,\beta_{n+1})\in\mathbb{N}^{n+1}$.

Then we find the expression

$$\partial^{\alpha'} t^{\beta'} \;=\; \partial^{\alpha} \partial_{n+1}^{\alpha_{n+1}} t^{\beta} t_{n+1}^{\beta_{n+1}} \;=\; \partial^{\alpha} t^{\beta}\, \partial_{n+1}^{\alpha_{n+1}} t_{n+1}^{\beta_{n+1}}$$

where we already used, that ∂_{n+1} is $R[t_1,\ldots,t_n]$-linear. If $\beta_{n+1} > \alpha_{n+1}$ then $\partial_{n+1}^{\alpha_{n+1}} t_{n+1}^{\beta_{n+1}} = 0$ by the case $n = 1$. In this case the whole term vanishes. And if $\beta_{n+1} \leq \alpha_{n+1}$ then by $n = 1$ again

$$\partial^{\alpha} t^{\beta}\, \partial_{n+1}^{\alpha_{n+1}} t_{n+1}^{\beta_{n+1}} \;=\; \partial^{\alpha} t^{\beta} \frac{\beta_{n+1}!}{(\beta_{n+1}-\alpha_{n+1})!}\, t_{n+1}^{\beta_{n+1}-\alpha_{n+1}}$$

Now insert the induction hypothesis for $\partial^{\alpha} t^{\beta}$: This either is 0, if there is some $i \in 1\ldots n$ with $\alpha_i > \beta_i$ such that the whole term vanishes, again. Or, in case $\alpha_i \leq \beta_i$ we compute

$$\partial^{\alpha'} t^{\beta'} \;=\; \prod_{i=1}^{n} \frac{\beta_i!}{(\beta_i-\alpha_i)!}\, t_i^{\beta_i-\alpha_i} \frac{\beta_{n+1}!}{(\beta_{n+1}-\alpha_{n+1})!}\, t_{n+1}^{\beta_{n+1}-\alpha_{n+1}} \;=\; \frac{\beta'!}{(\beta'-\alpha')!}\, t^{\beta'-\alpha'}$$

(iii) By (i) $R[\partial_1,\ldots,\partial_n]$ is generated by mutually commutative elements and hence is a commutative algebra in itself. And clearly $\varepsilon : f \mapsto f(\partial_1,\ldots,\partial_n)$ is a surjective homomorphism from the polynomial ring $R[d_1,\ldots,d_n]$ to $R[\partial_1,\ldots,\partial_n]$. It suffices to check that $\mathrm{kn}(\varepsilon) = 0$, then ε is injective and hence an isomorphism. So consider any $f \in R[d_1,\ldots,d_n]$ such that $f \neq 0$, then we need to show $f(\partial_1,\ldots,\partial_n) \neq 0$. We do this by induction on n once more: In case $n = 1$ let $m := \deg(f)$ be the degree of $f \in R[d_1]$, in particular $f[m] \neq 0$. Let use (ii) to evaluate what $f(\partial_1)$ makes out of t_1^m:

$$f(\partial_1)(t_1^m) \;=\; \sum_{k=0}^{m} f[k]\, \partial_1^k t_1^m \;=\; \sum_{k=0}^{m} f[k] \frac{m!}{(m-k)!} t_1^{m-k}$$

In particular the constant coefficient of $f(\partial_1)(t_1^m)$ is assumed for $k = m$ and this is $f[m] \cdot m! \neq 0$, which is non-zero, as R is an integral domain. Thus we find $f(\partial_1)(t_1^m) \neq 0$ hence $f(\partial_1) \neq 0$. Now to the induction step $n \geq 2$: If we have $f \in R[t_2,\ldots,t_n]$ then we are done by induction hypothesis. Otherwise, if f depends on t_1 let $m := \deg_1(f)$ and write $f \in R[d_1,\ldots,d_n]$ as an element of $R[d_2,\ldots,d_n][d_1]$, that is we write f in the form

$$f(d_1,\ldots,d_n) \;=\; \sum_{k=0}^{m} f_k(d_2,\ldots,d_n)\, t_1^k$$

for some $f_k \in R[d_2,\ldots,d_n]$ with $f_d \neq 0$. What works out once, works out twice: As $f_d \neq 0$ the induction hypothesis yields $f_d(\partial_2,\ldots,\partial_n) \neq 0$, that is there is some $g \in R[t_2,\ldots,t_n]$ such that $f_d(\partial_2,\ldots,\partial_n)(g) \neq 0$. Now take a look at

$$f(\partial_1,\ldots,\partial_n)(g t_1^m) \;=\; \sum_{k=0}^{m} f_k(\partial_2,\ldots,\partial_n)\partial_1^k(g t_1^m) \;=\; \sum_{k=0}^{m} f_k(\partial_2,\ldots,\partial_n)(g) \frac{m!}{(m-k)!} t_1^{m-k}$$

Again the constant term in t_1 is assumed for $k = m$ and is given to be $f(\partial_2,\ldots,\partial_2)(g) \cdot m!$. But $R[d_2,\ldots,d_n]$ is an integral domain, too and hence the constant term in t_1 of $f(\partial_1,\ldots,\partial_n)(g t_1^m)$ is non-zero. In particular $f(\partial_1,\ldots,\partial_n)(g t_1^m)$ cannot be zero and hence $f(\partial_1,\ldots,\partial_n) \neq 0$.

(iv) Let us first prove the chain rule for monomials $g(t) = t^{\alpha}$ where $\alpha = (\alpha_1,\ldots,\alpha_n)$. Let us also

abbreviate $f = (f_1, \ldots, f_n) \in R[t_1, \ldots, t_n]^n$. As $\partial/\partial s_i$ is a derivation we can use (7.70) to get

$$\begin{aligned}\frac{\partial}{\partial s_i} g(f) &= \frac{\partial}{\partial s_i} f^\alpha = \frac{\partial}{\partial s_i}\left(\prod_{j=1}^n f_j^{\alpha_j}\right) \\ &= \sum_{j=1}^n \frac{\partial}{\partial s_i}\left(f_j^{\alpha_j}\right) \cdot \prod_{k\neq j}^n f_k^{\alpha_k} \\ &= \sum_{j=1}^n \alpha_j \frac{\partial f_j}{\partial s_i} \cdot f_j^{\alpha_j - 1} \cdot \prod_{k\neq j}^n f_j^{\alpha_j}\end{aligned}$$

Now note that $\partial g/\partial t_j = \alpha_j t_j^{\alpha_j - 1} \prod_k t_k^{\alpha_k}$ where the sum runs over $k \in \{1, \ldots, n\} \setminus \{j\}$. That is we recognize that $\partial g/\partial t_j(f)$ is part of the expression above, in fact we see

$$\frac{\partial}{\partial s_i} g(f) = \sum_{j=1}^n \frac{\partial f_j}{\partial s_i} \cdot \frac{\partial g}{\partial t_j}(f)$$

That is, we have proved the claim for any monomial $g(t) = t^\alpha$. Also note that in case $\alpha_j = 0$ both, the formal derivative $\partial/\partial t_j$ and the summand containing α_j vanish and hence we did not bother to distinguish cases, even though $f_j^{\alpha_j - 1}$ is not well-defined, in this case. So it remains to verify the identity for arbitrary $g \in R[t_1, \ldots, t_n]$, but by R-linearity this can be reduced to the case of moninomials, using the following computation

$$\begin{aligned}\frac{\partial}{\partial s_i} g(f) &= \frac{\partial}{\partial s_i}\left(\sum_{\alpha\in\mathbb{N}^n} g[\alpha]\, f^\alpha\right) \\ &= \sum_{\alpha\in\mathbb{N}^n} g[\alpha]\, \frac{\partial}{\partial s_i}(f^\alpha) \\ &= \sum_{\alpha\in\mathbb{N}^n} g[\alpha] \sum_{j=1}^n \frac{\partial f_j}{\partial s_i} \cdot \frac{\partial t^\alpha}{\partial t_j}(f) \\ &= \sum_{j=1}^n \frac{\partial f_j}{\partial s_i} \cdot \left(\sum_{\alpha\in\mathbb{N}^n} g[\alpha] \frac{\partial t^\alpha}{\partial t_j}\right)(f) \\ &= \sum_{j=1}^n \frac{\partial f_j}{\partial s_i} \cdot \frac{\partial g}{\partial t_j}(f)\end{aligned}$$

(v) Let us first check the Taylor expansion for $x = 0$: Let us abbreviate $\forall\, i \in 1 \ldots n : \alpha_i \leq \beta_i$ by $\alpha \leq \beta$, then according to (ii) we have $\partial^\alpha t^\beta = 0$ for any β for which $\alpha \leq \beta$ is untrue. And for $\alpha \leq \beta$ we can use the formula for $\partial^\alpha t^\beta$ in (ii) and compute

$$\partial^\alpha f = \sum_{\beta\in\mathbb{N}^n} f[\beta]\,(\partial^\alpha t^\beta) = \sum_{\beta\geq\alpha} f[\beta]\, \frac{\beta!}{(\beta-\alpha)!}\, t^{\beta-\alpha}$$

From this we find $(\partial^\alpha f)(0) = \alpha! f[\alpha]$ as $\beta = \alpha$ is the only constant term in the expression for $\partial^\alpha f$. In particular we can write out f in the following way

$$f = \sum_{\alpha\in\mathbb{N}^n} f[\alpha]\, t^\alpha = \sum_{\alpha\in\mathbb{N}^n} \frac{1}{\alpha!}(\alpha! f[\alpha]) t^\alpha = \sum_{\alpha\in\mathbb{N}^n} \frac{1}{\alpha!}(\partial^\alpha f)(0)\, t^\alpha$$

For a general polynomial $f \in R[t_1,\dots,t_n]$ we use the automorphism $f(t) \mapsto f(t+x)$ on $R[t_1,\dots,t_n]$. If we take $g(t) := f(t+x)$ we can expand g at the point $x = 0$, that is

$$g(t) \;=\; \sum_{\alpha\in\mathbb{N}^n} \frac{1}{\alpha!}\big(\partial^\alpha g\big)(0)\, t^\alpha$$

By construction we have $f(t) = g(t-x)$ and hence can evaluate $f(t)$ in terms of the expansion of g at $x = 0$. Applying the inverse automorphism $g \mapsto g(t-x)$ we find

$$f(t) \;=\; g(t-x) \;=\; \sum_{\alpha\in\mathbb{N}^n} \frac{1}{\alpha!}\big(\partial^\alpha g\big)(0)\,(t-x)^\alpha$$

We need to take control of $(\partial^\alpha g)(0)$, still. So we use the chain rule (iv) with the parameters $g := f$, $f_j := t_j + x_j$ and $s_i := t_i$: Then we get the identifications $\partial g/\partial s_i(f)$ becomes $\partial_i f(t+x) = \partial_i g$ and $\partial f_j/\partial s_i$ becomes $\partial_i(t_j + x_j) = \delta_{i,j}$ and $\partial g/\partial t_j$ becomes $\partial_j f$ such that

$$(\partial_i g)(t) \;=\; \sum_{j=1}^{n} \delta_{i,j}(\partial_j f)(t+x) \;=\; (\partial_i f)(t+x)$$

By induction we find $(\partial^\alpha g)(t) = (\partial^\alpha f)(t+x)$ for any $\alpha \in \mathbb{N}^n$. And evaluating this identity at $t = x$ we get $(\partial^\alpha g)(0) = (\partial^\alpha f)(x)$ and thereby the general Taylor expansion

$$f(t) \;=\; \sum_{\alpha\in\mathbb{N}^n} \frac{1}{\alpha!}\big(\partial^\alpha f\big)(x)\,(t-x)^\alpha$$

□

Proof of (7.32):

(i) Let us regard the truncation homomorphism $\varrho : R[\![\varepsilon]\!] \twoheadrightarrow R[\![\varepsilon]\!]/\varepsilon^{l+1}R[\![\varepsilon]\!]$, where for any $a \in R[\![\varepsilon]\!]$ this is defined by $\varrho(a) := a + \varepsilon^{l+1}R[\![\varepsilon]\!]$. By assumption we have $\varrho(a_i) = \varrho(b_i)$ for any $i \in 1\dots n$ and hence for any polynomial $f \in R[t_1,\dots,t_n]$

$$\varrho(f(b_1,\dots,b_n)) \;=\; f(\varrho(b_1),\dots,\varrho(b_n)) \;=\; f(\varrho(a_1),\dots,\varrho(a_n)) \;=\; \varrho(f(a_1,\dots,a_n))$$

as ϱ commutes with additions and multiplications. Yet by construction of ϱ this means that for any $k \in 0\dots l$ we have $f(b_1,\dots,b_n)[k] = f(a_1,\dots,a_n)[k]$, as we had claimed.

(ii) We will first prove the identity of $f(a)$ which basically is a straightforward computation. Let us just write down what $f(a)$ means explicitly

$$f(a) \;=\; \sum_{\alpha\in\mathbb{N}^n} f[\alpha]\, a^\alpha \;=\; \sum_{\alpha\in\mathbb{N}^n} f[\alpha] \prod_{i=1}^{n} a_i^{\alpha_i}$$

Let us first consider polynomials $a_i \in R[\varepsilon]$ only and choose an $l \in \mathbb{N}$ such that $\deg(a_i) \le l$ for all $i \in 1\dots n$. Then we can write $a_i = a_i[0] + a_i[1]\varepsilon + \dots + a_i[l]\varepsilon^l$ and the polynomial rule (also called general binomial theorem) (1.41) yields the identity

$$a_i^{\alpha_i} \;=\; \big(a_i[l]\varepsilon^l + \dots + a_i[1]\varepsilon + a_i[0]\big)^{\alpha_i}$$

$$
\begin{aligned}
&= \sum_{|\beta_i|=\alpha_i} \binom{\alpha_i}{\beta_i} \prod_{k=0}^{l} \left(a_i[k]\varepsilon^k\right)^{\beta_{i,k}} \\
&= \sum_{|\beta_i|=\alpha_i} \binom{\alpha_i}{\beta_i} \left(\prod_{k=0}^{l} a_i[k]^{\beta_{i,k}}\right) \left(\prod_{k=0}^{l} \varepsilon^{k\cdot\beta_{i,k}}\right) \\
&= \sum_{|\beta_i|=\alpha_i} \binom{\alpha_i}{\beta_i} \dot{a}_i^{\beta_i} \varepsilon^{\|\beta_i\|}
\end{aligned}
$$

where we denoted $\dot{a}_i := (a_i[0], a_i[1], \ldots, a_i[l]) \in R^{l+1}$ the summation runs over all multi-indices $\beta_i = (\beta_{i,0}, \ldots, \beta_{i,l}) \in \mathbb{N}^{l+1}$ with $|\beta_i| = \beta_{i,0} + \cdots + \beta_{i,l} = \alpha_i$ and $\|\beta_i\| := 1 \cdot \beta_{i,1} + 2 \cdot \beta_{i,2} + \cdots + l \cdot \beta_{i,l}$. Inserting this identity into our expression for $f(a)$ we find

$$
f(a) \;=\; \sum_{\alpha\in\mathbb{N}^n} f[\alpha] \prod_{i=1}^{n} \sum_{|\beta_i|=\alpha_i} \binom{\alpha_i}{\beta_i} \dot{a}_i^{\beta_i} \varepsilon^{\|\beta_i\|}
$$

We refer to (1.41) again, where we have seen, that in arbitrary commutative rings R, for arbitrary elements $r_{i,\beta_i} \in R$ and any finite index sets B_i (where $i \in 1 \ldots n$) summation and multiplication can be interchanged in the following way

$$
\prod_{i=1}^{n} \sum_{\beta_i\in B_i} r_{i,\beta_i} \;=\; \sum_{\beta\in B_1\times\cdots\times B_n} \prod_{i=1}^{n} r_{i,\beta_i}
$$

In our case we have $B_i = \{\, \beta_i \in B \mid |\beta_i| = \alpha_i \,\}$ where $B := \mathbb{N}^{l+1}$ and hence the product is given to be $B(\alpha) := B_1 \times \cdots \times B_n = \{\, \beta \in B \mid |\beta| = \alpha \,\}$, such that we arrive at

$$
f(a) \;=\; \sum_{\alpha\in\mathbb{N}^n} f[\alpha] \sum_{\beta\in B(\alpha)} \prod_{i=1}^{n} \binom{\alpha_i}{\beta_i} a_i^{\beta_i} \varepsilon^{\|\beta_i\|}
$$

Contracting the product (over i) the binomial coefficients (α_i over β_i) multiply up to (α over β), the $(\dot{a}_i)^{\beta_i}$ multiply up to $(\dot{a})^{\beta}$ and the $\varepsilon^{\|\beta_i\|}$ multiply up to $\varepsilon^{\|\beta\|}$. Altogether we find that

$$
\begin{aligned}
f(a) \;&=\; \sum_{\alpha\in\mathbb{N}^n} f[\alpha] \sum_{\beta\in B(\alpha)} \binom{\alpha}{\beta} \dot{a}^{\beta} \varepsilon^{\|\beta\|} \\
&=\; \sum_{k=0}^{\infty} \left(\sum_{\alpha\in\mathbb{N}^n} \sum_{\beta\in B(\alpha,k)} \binom{\alpha}{\beta} f[\alpha]\, \dot{a}^{\beta} \right) \varepsilon^k \\
&=\; \sum_{k=0}^{\infty} \mathcal{L}_k(f)(\dot{a})\, \varepsilon^k
\end{aligned}
$$

That is we have proved the claim for polynomials $a_i \in R[\varepsilon]$. For general power series $a_i \in R[\![\varepsilon]\!]$ consider any $k \in \mathbb{N}$, all we have to prove is $f(a_1, \ldots, a_n)[k] = \mathcal{L}_k(f)(\dot{a})$. Yet by (i) we know that for $f(a_1, \ldots, a_n)[k]$ the coefficients $a_i[j]$ with $j > k$ are irrelevant. That is we may take to $b_i := a_i[0] + a_i[1]\varepsilon + \cdots + a_i[k]\varepsilon^k \in R[\varepsilon]$ instead. And for these polynomials we have just seen

$$
\begin{aligned}
f(a_1, \ldots, a_n)[k] \;&=\; f(b_1, \ldots, b_n)[k] \;=\; \mathcal{L}_k(f)(b[0], \ldots, b[k]) \\
&=\; \mathcal{L}_k(f)(a[0], \ldots, a[k]) \;=\; \mathcal{L}_k(f)(a[0], a[1], a[2], \ldots)
\end{aligned}
$$

(iii) Append R to a polynomial ring in the variable symbols $t_{r,s}$ where $r \in 1 \dots n$ and $s \in 0 \dots l$ and consider $a_r := t_{r,0} + t_{r,1}\varepsilon + \cdots + t_{r,l}\varepsilon^l \in R[\![\varepsilon]\!]$. Then by (ii) we have

$$f(a_1, \dots, a_n)(\varepsilon) \;=\; \sum_{k=0}^{\infty} \mathcal{L}_k(f)(a[0], \dots, a[l])\, \varepsilon^k$$

where as usual we took $a[k] := (a_1[k], \dots, a_n[k]) = (t_{1,k}, \dots, t_{n,k}) \in R^n$. Then by construction of the a_r we have $\mathcal{L}_k(f)(a[0], \dots, a[l]) = \mathcal{L}_k(f)$ and hence

$$\big(f \cdot g\big)(a_1, \dots, a_n) \;=\; \sum_{k=0}^{\infty} \mathcal{L}_k(f \cdot g)\, \varepsilon^k$$

But the evaluation of polynomials is a homomorphism, such that we may use the multiplicativity to split $(fg)(a_1, \dots, a_n)$ and evaluate separately

$$\begin{aligned}
& \big(f \cdot g\big)(a_1, \dots, a_n) \\
= \;& f(a_1, \dots, a_n) \cdot g(a_1, \dots, a_n) \\
= \;& \left(\sum_{i=0}^{\infty} \mathcal{L}_i(f)\, \varepsilon^i \right) \cdot \left(\sum_{j=0}^{\infty} \mathcal{L}_j(f)\, \varepsilon^j \right) \\
= \;& \sum_{k=0}^{\infty} \left(\sum_{i+j=k} \mathcal{L}_i(f) \cdot \mathcal{L}_j(g) \right) \varepsilon^k
\end{aligned}$$

Comparing the coefficients of ε^k we find the multiplicative identity of the claim. And the R-linearity is clear, as $\mathcal{L}_k$ has been defined by linear expansion of

$$t^\alpha \;\mapsto\; \sum_{\beta \in B(\alpha,k)} \binom{\alpha}{\beta}\, t^\beta$$

(iv) Consider any $\beta = (\beta_1, \dots, \beta_n) \in B(\alpha, l)$ and suppose t^β contains some factor of the form $t_{p,l}$ for some $p \in 1 \dots n$. As $t_{p,l}$ divides t^β we have $\beta_{p,l} \geq 1$ and hence $l = \|\beta\| \geq l \cdot \beta_{p,l} \geq l$. This implies $\beta_{p,l} = 1$ and we will argue below, that thereby β is of the form:

$$\begin{aligned}
\beta_i &= (\alpha_i, 0, 0, \dots) \text{ for any } i \neq p \text{ and} \\
\beta_p &= (\alpha_p - 1, 0, \dots, 0, 1, 0, \dots)
\end{aligned}$$

- If $j \notin \{1, l\}$ then $\beta_{p,j} = 0$, as any $\beta_{p,j} \geq 1$ would contribute $j \cdot \beta_{p,j}$ to $\|\beta\|$ and this already is at l, due to $l \cdot \beta_{p,l}$.
- $\beta_{p,0} \;=\; \alpha_i - 1$, as $|\beta_p| = \alpha_p$ and all the other $\beta_{p,j}$ have already been ruled out.
- If $i \neq p$ then $\beta_i \;=\; (\alpha_i, 0, \dots)$, as for any $j \geq 1$ any $\beta_{i,j} \geq 1$ would contribute $j \cdot \beta_{i,j}$ to $\|\beta\|$ and this already is at l, due to $l \cdot \beta_{p,l}$.

In particular we find (α_p over β_p) equals α_p and for $i \neq p$ we have (α_i over β_i) equals 1 instead. Combining this we get (α over β) equals α_p. Let us now split $B(\alpha, l)$ into two subsets

$$B'(\alpha, l) \;:=\; \Big\{ \beta \in B(\alpha, l) \mid \exists\, p \in 1 \dots n \,:\, t_{p,l} \mid t^\beta \Big\}$$

$$B''(\alpha,l) \;:=\; \Big\{\, \beta \in B(\alpha,l) \mid \forall\, p \in 1\dots n \,:\, t_{p,l} \not| \, t^\beta \,\Big\}$$

Now consider $f(\overline{a})[l]$, by (ii) this is $\mathcal{L}_l(f)(\dot{a})$ and we can split this term according to the disjoint union $B(\alpha,l) = B'(\alpha,l) \cup B''(\alpha,l)$ (where $\dot{a} = (a[0],\dots,a[l],0,\dots)$)

$$\mathcal{L}_l(f)(\dot{a}) \;=\; \underbrace{\sum_{\alpha\in\mathbb{N}^n} \sum_{\beta\in B'(\alpha,l)} \binom{\alpha}{\beta} f[\alpha]\, \dot{a}^\beta}_{\text{lead}} + \underbrace{\sum_{\alpha\in\mathbb{N}^n} \sum_{\beta\in B''(\alpha,l)} \binom{\alpha}{\beta} f[\alpha]\, \dot{a}^\beta}_{\text{rest}}$$

By what we have argued above, at the beginning of our proof ov (iv), $B'(\alpha,l)$ has exactly n elements that are determined by $\beta_p[l] = 1$ each, hence we get

$$\begin{aligned}
\text{lead} \;&=\; \sum_{\alpha\in\mathbb{N}^n} \sum_{p=1}^{n} \alpha_p f[\alpha]\, a_p[0]^{\alpha_p - 1} a_p[l] \prod_{i\neq p} a_i[0]^{\alpha_i} \\
&=\; \sum_{\alpha\in\mathbb{N}^n} f[\alpha] \sum_{p=1}^{n} \left(\partial_p \prod_{i=1}^{n} t_i^{\alpha_i} \right) (a[0]) \cdot a_p[l] \\
&=\; \sum_{p=1}^{n} \left(\partial_p \sum_{\alpha\in\mathbb{N}^n} f[\alpha]\, t^\alpha \right) (a[0]) \cdot a_p[l] \\
&=\; \sum_{p=1}^{n} (\partial_p f)(a[0]) \cdot a_p[l]
\end{aligned}$$

The rest does not contain any of the monomials $t_{i,l}$ and hence is independent of $a[l]$ and all higher orders $a[l+1],\dots$. That is we can arbitrarily change $a[l]$ without changing its value. In particular we may choose $a[l] = 0$, but if $a[l] = 0$ then any $\beta \in B'(\alpha,l)$ makes $\dot{a}^\beta = 0$ vanish, such that lead vanishes and only the rest remains

$$\text{rest} \;=\; \mathcal{L}_l(f)(a[0],\dots,a[l-1],0,0,\dots) \;=\; f(a)[l]$$

□

Proof of (7.75):

(i) *Uniqueness:* Suppose we have some $x \in \mathbb{R}$, such that $x^2 = r$. Then we can use this x to decompose $f(t) := t^2 - r \in \mathbb{R}[t]$ into $f(t) = t^2 - x^2 = (t+x)(t-x)$. Suppose $y > 0$ was another real number satisfying $y^2 = r$, then this would mean $f(y) = 0$ and thereby $t - y \mid f = (t+x)(t-x)$. But as $\mathbb{R}$ is a field, $\mathbb{R}[t]$ is an UFD and $t-y$, $t+x$ and $t-x$ all are prime, as they are of degree 1. Thus we have $t - y = t + x$ or $t - y = t - x$. The first would mean $y = -x$, but as $x > 0$ we have $-x < 0 < y$, so this is ruled out. So we are stuck with $t - y = t - x$ which means $x = y$, which is the uniqueness of the square root $x = \sqrt{r}$.

- *Monotony:* Consider real numbers $x, y \in \mathbb{R}$ such that $0 < x < y$. Multiplying this inequality with $x \geq 0$ we get $x^2 \leq xy$. And multiplying this inequality with $y \geq 0$ we get $xy \leq y^2$ which combines to $x^2 \leq y^2$. Now $x^2 = y^2$ would mean $x = y$, by uniqueness above. From this we conclude $x^2 < y^2$. Altogether we have found

$$0 < x < y \quad\Longrightarrow\quad x^2 < y^2$$

- *Convergence:* This proof uses some properties of the reals, that are best left to a course in numbers or analysis: Let us first prove, that for any $n \geq 0$ we have $0 < r \leq a_{n+1}^2$: To do this we simply employ the recursion formula and compute

$$a_{n+1}^2 - r \;=\; \frac{1}{4}\left(a_n + \frac{r}{a_n}\right)^2 - r \;=\; \left(a_n^2 + 2r + \frac{r^2}{a_n^2} - 4r\right)^2 \;=\; \frac{1}{4}\left(a_n - \frac{r}{a_n}\right)^2 \;\geq\; 0$$

Next we will prove that for any $1 \leq n \in \mathbb{N}$ we get $a_{n+1} < a_n$ by computing

$$a_n - a_{n+1} \;=\; a_n - \frac{1}{2}\left(a_n + \frac{r}{a_n}\right) \;=\; \frac{1}{2}\left(a_n - \frac{r}{a_n}\right) \;=\; \frac{a_n^2 - r}{2a_n} \;\geq\; 0$$

As we have seen $a_n^2 > r$ for any $n \geq 1$ we conclude $a_n - a_{n+1} \geq 0$ such that $r \leq a_{n+1} \leq a_n$. That is (a_n) is monotonously decreasing and bounded from below. In $\mathbb{R}$ this implies that (a_n) converges. Let $x \in \mathbb{R}$ be the limit of (a_n), then we have to prove $x^2 = r$. As $0 < r \leq (a_n)$ we have $0 < r \leq x$ and as $x \neq 0$ we may compute

$$x \;=\; \lim_{n\to\infty} a_n \;=\; \lim_{n\to\infty} a_{n+1} \;=\; \lim_{n\to\infty} \frac{1}{2}\left(a_n + \frac{r}{a_n}\right) \;=\; \frac{1}{2}\left(x + \frac{r}{x}\right)$$

Multiplying this equation by $2x$ we get $2x^2 = x^2 + r$ which turns into $x^2 = r$. By construction any a_n is contained in $\mathbb{Q}$, that is we have found a sequence in $\mathbb{Q}$, that converges and hence is a Cauchy-sequence. As $\mathbb{R}$ is complete, this means $x = (a_n) + \mathfrak{z}$ is a real number.

(ii) As $z \neq 0$ we have $r > 0$ and thereby (i) tells us there is a uniquely determined $x > 0$ with $x^2 = r$. This x is denoted by $x = \sqrt{r}$. In the following computation we make use of the *angle sum formula* (■) that are elementary to prove, but which we leave to standard textbooks on analysis

$$\begin{aligned} & \left(\pm\sqrt{r}\left(\cos\left(\frac{\alpha}{2}\right) + i \cdot \sin\left(\frac{\alpha}{2}\right)\right)\right)^2 \\ = \;& \sqrt{r}^2\left(\cos\left(\frac{\alpha}{2}\right)^2 - \sin\left(\frac{\alpha}{2}\right)\right) + 2i\sin\left(\frac{\alpha}{2}\right)\cos\left(\frac{\alpha}{2}\right) \\ = \;& r\left(\cos\left(\frac{\alpha}{2} + \frac{\alpha}{2}\right) + i\sin\left(\frac{\alpha}{2} + \frac{\alpha}{2}\right)\right) \;=\; z \end{aligned}$$

That is we have $w_1^2 = z$ and $w_2^2 = z$. Suppose we had $w_1 = w_2$, as also $w_1 = -w_2$ this would imply $w_2 = -w_2$ such that $2w_2 = 0$. But as $r > 0$ we have $w_2 \neq 0$ and thereby $2w_2 \neq 0$. Hence $w_1 \neq w_2$ are distinct. Thus the polynomial $f(t) := t^2 - z$ has the roots $\mathbb{V}(f) = \{w_1, w_2\}$. As $\mathbb{C}$ is an integral domain (even a field) the number of roots cannot exceed the degree of f, thus w_1 and w_2 are the only solutions of $w^2 = z$ - that is they are uniquely determined.

□

Proof of (7.76):

- We will evade the ordeal of proving all the properties of a commutative ring of $R[\sqrt{s}]$ by proving the first isomorphy: As always R^2 becomes an R-module under the operations $(a,b) + (c,d) = (a+c, b+d)$ and $a(c,d) = (ac, ad)$. And $R[t]/\mathfrak{w}$ becomes an R-module under the operations $(a + bt + \mathfrak{w}) + (c + dt + \mathfrak{w}) = (a+c) + (b+d)t + \mathfrak{w}$ and $a(c + dt + \mathfrak{w}) = ac + adt + \mathfrak{w}$. From

this it is clear, that the following map is a well-defined and R-linear

$$\Phi \,:\, R[\sqrt{s}] \,\to\, {R[t]}\Big/_{\mathfrak{w}} \,:\, (a,b) \,\mapsto\, a+tb+\mathfrak{w}$$

We will show, that this map is bijective, starting with the surjectivity: That is we consider any polynomial $f \in R[t]$ and need to find a, $b \in R$, such that $a+bt+\mathfrak{w} = f+\mathfrak{w}$. To do this we use the identity $t^2+\mathfrak{w} = s+\mathfrak{w}$ and split f into its odd and even powers

$$\begin{aligned} f+\mathfrak{w} \;&=\; \sum_{n=0}^{\infty} f[n]\,t^n + \mathfrak{w} \;=\; \sum_{j=0}^{\infty} f[2j]\,t^{2j} + t\cdot\sum_{k=0}^{\infty} f[2k+1]\,t^{2k} + \mathfrak{w} \\ &=\; \underbrace{\sum_{j=0}^{\infty} f[2j]\,s^j}_{a} + t\cdot\underbrace{\sum_{k=0}^{\infty} f[2k+1]\,s^k}_{b} + \mathfrak{w} \end{aligned}$$

Thus if we take a and b as indicated above, we found $\Phi(a+b\omega) = f+\mathfrak{w}$ which is the surjectivity of the map Φ. Let us turn our attention to the injectivity: For this we consider $\Phi(a+b\omega) = 0$ which is $a+bt \in \mathfrak{w} = (t^2-s)R[t]$. That is there is some polynomial $f \in R[t]$ such that

$$a+tb \;=\; (t^2-s)f \;=\; \sum_{k=2}^{\infty} f[k-2]\,t^k - \sum_{k=0}^{\infty} sf[k]\,t^k$$

Comparing the degree 0 and 1 coefficients, we get $a = -sf[0]$ and $b = -sf[1]$ respectively. For the k-th coefficient, where $k \geq 2$ we find $0 = f[k-2] - sf[k]$, that is $sf[k] = f[k-2]$. In other words $sf[2] = f[0]$, $sf[3] = f[1]$, $sf[4] = f[2]$ and so on. Inductively we see $s^k f[2k] = f[0]$ and $s^k f[2k+1] = f[1]$ for any $k \in \mathbb{N}$. Multiplying these equations with $-s$ we find

$$-s^{k+1}f[2k] \;=\; a \quad\text{and}\quad -s^{k+1}f[2k+1] \;=\; b$$

As f is a polynomial, we may take $k > \deg(f)/2$ to find $f[2k] = 0$ and $f[2k+1] = 0$ from which we get $a = 0$ and $b = 0$. That is $a+b\omega = 0$ and this also implies the injectivity of Φ. Altogether Φ is an isomorphism of R-modules.

- We now use this isomorphism compare the multiplication of $R[\sqrt{s}]$ and $R[t]/\mathfrak{w}$. The multiplication of $R[\sqrt{s}]$ is given to be $(a+b\omega)(c+d\omega) = (ac+bds)+(ad+bc)\omega$. And if we take a look at the multiplication of $R[t]/\mathfrak{w}$ we find

$$\big(a+tb+\mathfrak{w}\big)\big(c+dt+\mathfrak{w}\big) \;=\; ac+\big(ad+bc\big)t+bdt^2+\mathfrak{w} \;=\; \big(ac+dbs\big)+\big(ad+bc\big)t+\mathfrak{w}$$

That is $(a+b\omega)(c+d\omega)$ is mapped to $(a+tb+\mathfrak{w})(c+dt+\mathfrak{w})$ under Φ. That is Φ not only is R-linear and bijective, but respects the multiplication, as well. In particular Φ links the unit elements $1 = (1,0) \mapsto 1+\omega$. Thus $R[\sqrt{s}]$ inherits all the properties (associativity, commutativity and distributivity) of the multiplication from $R[t]/\mathfrak{w}$ and thereby is an R-algebra.

- Clearly $(a+b\omega)(a-b\omega) = a^2-b^2\omega^2 = a^2-sb^2$. Suppose $u := a^2-sb^2 \in R^*$ is a unit of R,

then combining these properties, we find

$$(a+b\omega)\Big(u^{-1}(a-b\omega)\Big) \;=\; (a+b\omega)(a-b\omega)u^{-1} \;=\; uu^{-1} \;=\; 1$$

Thus we find that $u = a^2 - sb^2 \in R^*$ implies $a+b\omega$ to be a unit of $R[\sqrt{s}]$, with inverse element $u^{-1}(a-b\omega)$. Conversely suppose $a+b\omega$ is a unit, that is there is some $c+d\omega \in R[\sqrt{s}]$ such that

$$1 \;=\; (a+b\omega)(c+d\omega) \;=\; (ac+dbs) + (ad+bc)\omega$$

That is we have $ac+dbs = 1$ and $ad+bc = 0$. Let again $u := a^2 - sb^2 \in R$, if we multiply the equation $1 = (a+b\omega)(c+d\omega)$ by $a-b\omega$, then we get

$$a - b\omega \;=\; (a-b\omega)(a+b\omega)(c+d\omega) \;=\; u(c+d\omega)$$

That is we have $a = uc$ and $b = -ud$. Multiplying the first equation with c and the second with ds we find $ac = uc^2$ and $bds = -ud^2s$ such that $1 = ac+bds = uc^2 - ud^2s = u(c^2 - ud^2)$. From this we find that $u \in R$ is a unit of R. That is we also have the inclusion of $R[\sqrt{s}]^*$ into $\{\, a+b\omega \mid a^2 - sb^2 \,\}$ and hence these sets are equal.

- It remains to verify the embedding of $R[\sqrt{s}] = \{\, a+b\omega \mid a,b \in R \,\}$ into the ring of 2×2-matrices over R. It is clear that the map given in the claim is well-defined and injective. Also - as the addition and scalar multiplication on R^2 and $\mathrm{mat}_2(R)$ are component-wise - this map is R-linear and $1 = 1+0\omega \mapsto \mathbb{1}_2$ is trivial. So it only remains to verify its multiplicativity: Let us compute

$$\begin{pmatrix} a & b \\ sb & a \end{pmatrix}\begin{pmatrix} c & d \\ sd & c \end{pmatrix} \;=\; \begin{pmatrix} ac+sbd & ad+bc \\ sbc+sad & sbd+ac \end{pmatrix}$$

 We see that the product matrix is precisely the image of $(ac+sbd)+(ad+bc)\omega = (a+b\omega)(c+d\omega)$, which is the multiplicativity we were looking for.

□

Proof of (7.77):
First note that $2^2 = (1+1)(1+1) = 1+1+1+1 = 4$ in general rings. Then the identity $at^2+bt+c = a(t+b/2a)^2 - \Delta/4a$ is straightforward to see. All we have to do is evaluate the binomial and recall $\Delta = b^2 - 4ac$. This is all due to the commutativity of the base ring R

$$a\left(t+\frac{b}{2a}\right)^2 - \frac{\Delta}{4a} \;=\; a\left(t^2+\frac{b}{a}t+\frac{b^2}{4a^2}\right)^2 - \frac{\Delta}{4a} \;=\; at^2+bt+\frac{b^2}{4a} - \frac{b^2-4ac}{4a} \;=\; at^2+bt+c$$

Now, suppose f had a root $x \in R$, that is $f(x) = 0$. Then this would imply $\Delta/4a = a(x^2+b/2a)^2$. Multiplying this equation by $4a$ it would turn into an expression that is a square in R

$$\Delta \;=\; 4a^2\left(x+\frac{b}{2a}\right)^2 \;=\; (2a)^2\left(x+\frac{b}{2a}\right)^2 \;\in\; R^\square$$

Conversely suppose $\Delta = \omega^2 \in R^\square$ is a square in R, then we can use the vertex form of f to turn it into

a product of two linear factors. The factor form of f is obvious from the following identity

$$\frac{f(t)}{a} \;=\; \left(t+\frac{b}{2a}\right)^2 - \frac{\Delta}{4a^2} \;=\; \left(t+\frac{b}{2a}\right)^2 - \left(\frac{\omega}{2a}\right)^2 \;=\; \left(t+\frac{b}{2a}+\frac{\omega}{2a}\right)\left(t+\frac{b}{2a}-\frac{\omega}{2a}\right)$$

In particular $\Delta \in R^\square$ is equivalent to f having roots in R. If R is an integral domain, then f can have at most $\deg(f) = 2$ roots, because of (7.54.(iv)). And if $\Delta = \omega^2$ for some $\omega \neq 0$ we already see two distinct roots, given in the claim of $\mathbb{V}(f)$, in the factor form of f

$$f(t) \;=\; a\left(t-\frac{-b-\omega}{2a}\right)\left(t-\frac{-b+\omega}{2a}\right)$$

And if $\Delta = 0$, then the vertex form tells us $f = a(t+b/2a)^2$. Now consider any root $x \in R$ of f, that is $0 = (x+b/2a)^2$. If R is an integral domain, then we conclude $x = -b/2a$. That is the root of f is uniquely determined to be $-b/2a$ which is the above formula for $\omega = 0$. □

Proof of (7.79):

(i) If $z = a+ib \in \mathbb{C}$ is any complex number, then $\overline{z} = a-ib$ by definition. Thus we see $z+\overline{z} = 2a \in \mathbb{R}$ and $z\overline{z} = (a+ib)(a-ib) = a^2-(ib)^2 = a^2+b^2 \in \mathbb{R}$. Now let $n := \deg(f)$, then from this it is obvious, that

$$f+\overline{f} \;=\; \sum_{k=0}^{n} f[k]\,t^k + \sum_{k=0}^{n} \overline{f[k]}\,t^k \;=\; \sum_{k=0}^{n} \Big(f[k]+\overline{f[k]}\Big)\,t^k \;\in\; \mathbb{R}[t]$$

Now consider $w = u+iv \in \mathbb{C}$, then $(a-ib)(u-iv) = (au-bv)-i(av+bu)$, that is $\overline{w\cdot z} = \overline{w}\cdot\overline{z}$. In particular we get $\overline{z^k} = \overline{z}^k$ for any $k \in \mathbb{N}$. And with this we are able to compute

$$f(\overline{z}) \;=\; \sum_{k=0}^{n} f[k]\,\overline{z}^k \;=\; \sum_{k=0}^{n} \overline{\overline{f[k]}}\,\overline{z^k} \;=\; \overline{\sum_{k=0}^{n} \overline{f[k]}\,z^k} \;=\; \overline{\overline{f}(z)}$$

Conjugating this identity again, we get $\overline{f(\overline{z})} = \overline{f}(z)$, as claimed. Let us finally prove $f\overline{f} \in setR[t]$, by induction on n: If $f = 0$, then $f\overline{f} = 0$, too, such that there is nothing to prove. For $n = 0$ we have $f = z$ for some $z \in \mathbb{C}$. Then $f\overline{f} = z\overline{z} \in \mathbb{R}$, by the above. For the induction step we write $f = f[n]\,t^n + r(t)$, where $r \in \mathbb{C}[t]$ is of degree $\deg(r) \leq n-1$. Then $\overline{f} = \overline{f[n]}\,t^n + \overline{r}$ and thereby

$$f\overline{f} \;=\; \big(f[n]\,t^n + r(t)\big)\left(\overline{f[n]}\,t^n + \overline{r}(t)\right) \;=\; f[n]\overline{f[n]}\,t^{2n} + \Big(f[n]\,\overline{r}(t) + \overline{f[n]}\,r(t)\Big)\,t^n + r\overline{r}$$

Hereby $f[n]\overline{f[n]} \in \mathbb{R}$ is clear again, by the above. And $r\overline{r} \in \mathbb{R}[t]$ is true, by induction hypothesis. It remains to prove, that the middle term is a polynomial over the reals, as well. So let us take a closer look:

$$\begin{aligned} f[n]\,\overline{r}(t) + \overline{f[n]}\,r(t) \;&=\; \sum_{k=0}^{n-1} \Big(f[n]\,\overline{f[k]} + \overline{f[n]}\,f[k]\Big)\,t^k \\ &=\; \sum_{k=0}^{n-1} \Big(f[n]\,\overline{f[k]} + \overline{f[n]\,\overline{f[k]}}\Big)\,t^k \end{aligned}$$

So if we let $s[k] := f[n]\,\overline{f[k]} \in \mathbb{C}$ then the coefficients of this polynomial are given to be $s[k]+\overline{s[k]} \in$

$\mathbb{R}$ and thereby the middle term is a polynomial in $\mathbb{R}[t]$, as well. And from this we finally get $f\overline{f} \in \mathbb{R}[t]$.

(ii) The proof is analytic in nature and hence we only try to get the idea across and not fill in every technical detail. We use standard arguments of a course in analysis of one real variable (■) : Let $n := \deg(p) = 2m+1$, then the leading coefficient $p[n] \neq 0$ is non-zero. Without loss of generality we may assume $p[n] > 0$: If not we could find a root x of $-p$, which also is a root of p. We consider $p \in \mathbb{R}(t)$ and use this to divide p by t^n. We also pull out $p[n]$, that is we rewrite p in the form

$$\frac{p(t)}{t^n} \;=\; \frac{1}{t^n}\sum_{k=0}^{n} p[k]\,t^k \;=\; p[n]\left(1+\sum_{k=0}^{n-1}\frac{p[k]}{p[n]}\,\frac{1}{t^{n-k}}\right)$$

In the limit $x \to \pm\infty$ the terms $1/x^{n-k} \to 0$ vanish so $p(x)/x^n$ converges to $p[n]$. And as $p(x)/x^n$ converges to $p[n]$, $p(x)$ has to stick to $p[n]\,x^n$ as x tends to $\pm\infty$. But as $n \geq 1$ and n is odd, we have $x^n \to \pm\infty$ for $x \to \pm\infty$. Altogether we conclude

$$\lim_{x\to\pm\infty} p(x) \;=\; \lim_{x\to\pm\infty} p[n]\,x^n \;=\; \pm\infty$$

That is there is some $r > 0$ such that $p(-r) < 0 < p(r)$. As p is continuous there has to be some $x \in \mathbb{R}$ with $-r < x < r$ such that $p(x) = 0$ and this is just what we sought for.

(iii) Let us first regard the case of a monic polynomial $p \in \mathbb{R}[t]$ over the reals, such that $n := \deg(p) \geq 1$. We claim, that $p(z) = 0$ for some $z \in \mathbb{C}$. Write $n = 2^k m$ for some $k \in \mathbb{N}$ and $1 \leq m \in \mathbb{N}$ such that m is odd. We prove the claim by induction on k: If $k = 0$, then $n = m \geq 1$ is odd and thereby even $p(x) = 0$ for some $x \in \mathbb{R}$, due to (ii). Now for the induction step:

By (8.10.(iv)) there is some field K such that $K : \mathbb{C}$ is a finite field extension and p splits over K. That is there are $z_1, \ldots, z_n \in K$, such that p can be written, as

$$p \;=\; (t-z_1)\ldots(t-z_n) \;=\; t^n - a_1 t^{n-1} + \cdots + a_{n-1}t + a_n$$

As $p \in \mathbb{R}[t]$ we have $a_i \in \mathbb{R}$ and we could even express the a_i in terms of elementary symmetric polynomials in the z_i. Whatever, let $R := \mathbb{R}[t]$ and fix any $a \in \mathbb{R}$. Then we define another monic polynomial $s_a \in R[t_1, \ldots, t_n]$, this time

$$s_a(t_1, \ldots, t_n) \;=\; \prod_{1\leq i<j\leq n} \big(t - (t_i + t_j) - a t_i t_j\big)$$

Obviously s_a is symmetric and hence by (7.67.(iv)) there is some polynomial $h \in R[t_1, \ldots, t_n]$ such that s_a satisfies the identity

$$s_a(z_1, \ldots, z_n) \;=\; h(a_1, \ldots, a_n) \;=:\; g_a(t) \;\in\; \mathbb{R}[t]$$

That is $g_a \in \mathbb{R}[t]$ and $s_a(z_1, \ldots, z_n) \in K[t]$ have the same degree and share the same coefficients. So let us take a look at the degree of $s_a(z_1, \ldots, z_n)$. By construction we have

$$\deg\big(s_a(z_1, \ldots, z_n)\big) \;=\; \sum_{1\leq i<j\leq n} 1 \;=\; \frac{n(n-1)}{2} \;=\; \frac{2^k m(n-1)}{2} \;=\; 2^{k-1}m(n-1)$$

As $k \geq 1$ we find n to be even, such that $n-1$ is odd. This makes $m(n-1)$ odd, too. Therefore we can use the induction hypothesis on g_a which means that there is some $z_a \in \mathbb{C}$ such that $g_a(z_a) = 0$. Take a look at the expression behind

$$0 \;=\; g_a(z_a) \;=\; s_a(z_1,\ldots,z_n)(z_a) \;=\; \prod_{1\leq i<j\leq n} \big(z_a - (z_i+z_j) - az_iz_j\big)$$

As K is a field and hence an integral domain this means that one of the factors has to be zero. Time to summarize what we have got so far: For any $a \in \mathbb{R}$ there is some $z_a \in \mathbb{C}$ such that for some $i, j \in 1\ldots n$ with $i < j$ we get the equation

$$z_a - (z_i + z_j) - az_iz_j \;=\; 0$$

As $\mathbb{R}^*$ is infinite and there only are finitely many (i,j) with $1 \leq i < j \leq n$ there have to be two distinct $a \neq b \in \mathbb{R}^*$ that belong to the same pair (i,j). That is

$$\begin{aligned} z_a &= z_i + z_j + az_iz_j \\ z_b &= z_i + z_j + bz_iz_j \end{aligned}$$

Subtracting these equations, we get $z_b - z_a = (b-a)z_iz_j$ and as $b - a \neq 0$ this can be turned into $z_iz_j = (a_b - z_a)(b-a)^{-1} \in \mathbb{C}$. And multiplying the first equation by b, the second with a and subtracting we also find $bz_a - az_b = (b-a)(z_i+z_j)$ which turns into $z_i + z_j = (bz_a - az_b)(b-a)^{-1} \in \mathbb{C}$. Altogether we have both $z_i + z_j$ and $z_iz_j \in \mathbb{C}$ and thereby

$$(t-z_i)(t-z_j) \;=\; t^2 - (z_i+z_j)t + z_iz_j \;\in\; \mathbb{C}[t]$$

That is z_i and z_j are the roots of a quadratic polynomial polynomial of $\mathbb{C}[t]$. But by (7.77) the roots of such a polynomial are uniquely determined elements of $\mathbb{C}$. That is z_i and $z_j \in \mathbb{C}$ themselves and in particular $p(z_i) = 0$ for some $z_i \in \mathbb{C}$.

It remains to prove the general case $f \in \mathbb{C}[t]$ where $n = \deg(f) \geq 1$. In this case $p := f\overline{f} \in \mathbb{R}[t]$ is a polynomial over the reals of degree $2n \geq 1$. By what we have argued above, there is some $z \in \mathbb{C}$ such that $p(z) = 0$ and by construction that is $f(z)\overline{f}(z) = 0$. As $\mathbb{C}$ is a field we conclude $f(z) = 0$ (which is what we wanted) or $\overline{f}(z) = 0$. In the latter case (i) tells us $\overline{f(\overline{z})} = 0$ such that $f(\overline{z}) = 0$. That is $\overline{z} \in \mathbb{C}$ is a root of f, which is good enough for the claim to be true.

□

Proof of (3.89):
Let us start with (a) $\implies$ (b): By assumption we have $\alpha : M \to L$ such that $\alpha\varphi = \mathbb{1}_L$. Let us consider any $x \in M$. Then $\alpha(x - \varphi\alpha(x)) = \alpha(x) - \alpha\varphi\alpha(x) = \alpha(x) - \alpha(x) = 0$. That is $x - \varphi\alpha(x) \in \ker(\alpha)$ and as $\varphi\alpha(x) \in \operatorname{im}(\varphi)$ also $x \in \ker(\alpha) + \operatorname{im}(\varphi)$. As $x \in M$ has been arbitrary this means $M = \ker(\alpha) + \operatorname{im}(\varphi)$. Now suppose we had $x \in \ker(\alpha) \cap \operatorname{im}(\varphi)$, say $x = \varphi(u)$, then $0 = \alpha(x) = \alpha\varphi(u) = u$ such that $x = \varphi(u) = \varphi(0) = 0$. That is $\ker(\alpha) \cap \operatorname{im}(\varphi) = 0$. So together we have proved

$$M \;=\; \ker(\alpha) \oplus \operatorname{im}(\varphi)$$

We are on the way to construct $\omega : N \to M$, so now consider $x, y \in M$ with $\psi(x) = \psi(y)$. Then we have $0 = \psi(x) - \psi(y) = \psi(x - y)$ such that $x - y \in \ker(\psi) = \operatorname{im}(\varphi)$. But of course $\varphi\alpha(y - x) \in \operatorname{im}(\varphi)$, too such that

$$(x - y) + \varphi\alpha(y - x) \ \in \ \operatorname{im}(\varphi)$$

Yet $(x - y) + \varphi\alpha(y - x) = x - y + \varphi\alpha(y) - \varphi\alpha(x) = (x - \varphi\alpha(x)) - (y - \varphi\alpha(y))$ and as we have seen above $x - \varphi\alpha(x)$ and $y - \varphi\alpha(y) \in \ker(\alpha)$. Therefore we also find that

$$(x - y) + \varphi\alpha(y - x) \ = \ (x - \varphi\alpha(x)) - (y - \varphi\alpha(y)) \ \in \ \ker(\alpha)$$

Together this is $(x - \varphi\alpha(x)) - (y - \varphi\alpha(y)) \in \operatorname{im}(\varphi) \cap \ker(\alpha) = 0$ such that $\psi(x) = \psi(y)$ implies $x - \varphi\alpha(x) = y - \varphi\alpha(y)$. Note however, that ψ is surjective by assumption, so for any $p \in N$ there is some $x \in M$ such that $p = \psi(x)$. And thereby we may finally define

$$\omega(p) \ := \ x - \varphi\alpha(x) \ \text{ for some } x \in M \text{ with } \psi(x) = p$$

This is well defined, as the result of $\omega(p)$ does not depend on the actual choice of x, as we have just argued. And as both ψ and $\mathbb{1}_M - \varphi\alpha$ are homomorphisms, so is ω. Now it is easy to compute $\psi\omega(p) = \psi(x - \varphi\alpha(x)) = \psi(x) - \psi\varphi\alpha(x) = \psi(x) - 0\alpha(x) = \psi(x) = p$ such that $\psi\omega = \mathbb{1}_N$. Thus we have arrived at (b).

The proof of (b) $\implies$ (a) is rather analogous: We have $\omega : N \to M$ such that $\psi\omega = \mathbb{1}_N$ and need to construct $\alpha : M \to L$. Given $x \in M$ we see $\psi(x - \omega\psi(x)) = \psi(x) - \psi\omega\psi(x) = \psi(x) - \psi(x) = 0$ such that $x - \omega\psi(x) \in \ker(\psi)$. And as $\omega\psi(x) \in \operatorname{im}(\omega)$ this is $x \in \ker(\psi) + \operatorname{im}(\omega)$. As x has been arbitrary we have found $M = \ker(\psi) + \operatorname{im}(\omega)$ again. Now suppose $x \in \ker(\psi) \cap \operatorname{im}(\omega)$, say $x = \omega(p)$ for some $p \in N$. Then $0 = \psi(x) = \psi\omega(p) = p$ such that $x = \omega(p) = \omega(0) = 0$. That is we also have $\ker(\psi) \cap \operatorname{im}(\omega) = 0$ again and thereby

$$M \ = \ \ker(\psi) \oplus \operatorname{im}(\omega)$$

We are on the way to construct $\alpha : M \to L$, as we have seen for any $x \in M$ we have $x - \omega\psi(x) \in \ker(\psi) = \operatorname{im}(\varphi)$. And as φ is injective by assumption there is a uniquely determined $u \in L$ such that $\varphi(u) = x - \omega\psi(x)$. Thus we may define

$$\alpha(x) \ := \ u \ \text{ where } u \in L \text{ with } \varphi(u) = x - \omega\psi(x)$$

As both φ and $\mathbb{1}_M - \omega\psi$ are homomorphisms, so is α. It remains to verify $\alpha\varphi = \mathbb{1}_L$. Thus consider any $u \in L$ and let $x := \varphi(u)$. Then $x - \omega\psi(x) = \varphi(u) - \omega\psi\varphi(u) = \varphi(u) - \omega 0(u) = \varphi(u)$. That is we have $\alpha(x) = u$ by definition of α, but this again is $\alpha\varphi(u) = u$ as needed. Thus we have arrived at (a), together we have (a) $\iff$ (b).

Now that the equivalence of (a) and (b) has been established, we will prove that $\ker(\alpha) = \operatorname{im}(\alpha)$ is in fact the same sub-module: We have seen that M can be decomposed into the inner direct sums

$$\begin{aligned} M &= \ker(\alpha) \oplus \operatorname{im}(\varphi) \\ M &= \operatorname{im}(\omega) \oplus \ker(\psi) \end{aligned}$$

But thereby $L' := \mathrm{im}(\varphi) = \mathrm{kn}(\psi)$ is precisely the same set. Thus the inner direct sums gives rise to the following isomorphisms

$$\begin{array}{rcl} \mathrm{kn}(\alpha) & \xrightarrow{\sim} & M \Big/ L' \ : \ k \mapsto k + L' \\ \mathrm{im}(\omega) & \xrightarrow{\sim} & M \Big/ L' \ : \ j \mapsto j + L' \end{array}$$

Composing these isomorphisms $k \mapsto k + L' \mapsto k$ we find that the identity map is an isomorphism from $\mathrm{kn}(\alpha)$ to $\mathrm{im}(\omega)$. But the identity maps $\mathrm{kn}(\alpha)$ to itself so we have $\mathrm{im}(\omega) = \mathrm{kn}(\alpha)$.

The implication (c) $\implies$ (a) and (b) is rather easy: Let us denote the canonical homomorphisms $\pi_L : L \oplus N \to L$ given by $\pi_L(u,p) := u$ and $\iota_L : L \to L \oplus N$ given by $\iota_L(u) := (u,0)$. Likewise $\pi_N : L \oplus N \to N$ and $\iota_N : N \to L \oplus N$. If we have the isomorphism $\Phi : M \xrightarrow{\sim} L \oplus N$ then we may explicitly define $\alpha : M \to L$ and $\omega : N \to M$ to be

$$\begin{array}{rcl} \alpha & := & \pi_L \Phi \\ \omega & := & \Phi^{-1} \iota_N \end{array}$$

Recall that we have the commutativity of the diagram, that is $\Phi\varphi = \iota_L$ and $\pi_N \Phi = \psi$. Then for any $u \in L$ it is clear that $\alpha\varphi(u) = \pi_L \Phi \varphi(u) = \pi_L \iota_L(u) = u$. And likewise $\pi_N \Phi = \psi$ turns into $\pi_N = \psi \Phi^{-1}$ such that for any $p \in N$ we have $\psi\omega(p) = \psi\Phi^{-1}\iota_N(p) = \pi_N \iota_N(p) = p$. Thus α and ω satisfy the required properties and we have (a) and (b).

It remains to verify (a) and (b) $\implies$ (c): Again this can be done explicitly, given α let us define

$$\Phi \ : \ M \to L \oplus N \ : \ x \mapsto \big(\alpha(x), \psi(x)\big)$$

Clearly Φ is a homomorphism and we also find the commutativity of the diagram: For any $u \in L$ we get $\Phi\varphi(u) = (\alpha\varphi(u), \psi\varphi(u)) = (u,0) = \iota_L(u)$. And for any $x \in M$ we have $\pi_N \Phi(x) = \pi_N(\alpha(x), \psi(x)) = \psi(x)$. The inverse of Φ is given to be

$$\Phi^{-1} \ : \ L \oplus N \to M \ : \ (u,p) \mapsto \varphi(u) + \omega(p)$$

Let us verify, that this truly is the inverse: Starting with $x \in M$ we decompose $x = k + \ell$ for some $k \in \mathrm{kn}(\alpha) = \mathrm{im}(\omega)$ and $\ell \in \mathrm{im}(\varphi) = \mathrm{kn}(\psi)$. That is we may choose $u \in L$ and $p \in N$ such that $k = \omega(p)$ and $\ell = \varphi(u)$. Then

$$\begin{array}{rcl} \Phi^{-1}\Phi(x) & = & \varphi\alpha(x) + \omega\psi(x) \\ & = & \varphi\alpha(k+\ell) + \omega\psi(k+\ell) \\ & = & \varphi\alpha(\ell) + \omega\psi(k) \\ & = & \varphi\alpha\varphi(u) + \omega\psi\omega(p) \\ & = & \varphi(u) + \omega(p) \ = \ \ell + k \ = \ x \end{array}$$

Conversely for $u \in L$ and $p \in N$ then the composition of Φ after Φ^{-1} yields

$$\Phi\Phi^{-1}(u,p) \ = \ \big(\alpha\big(\varphi(u) + \omega(p)\big), \psi\big(\varphi(u) + \omega(p)\big)\big)$$

As $\omega(p) \in \mathrm{im}(\omega) = \mathrm{kn}(\alpha)$ and $\varphi(u) \in \mathrm{im}(\varphi) = \mathrm{kn}(\psi)$ we can drop $\omega(p)$ in α and likewise $\varphi(u)$ in ψ. It only remains the identity desired

$$\Phi\Phi^{-1}(u,p) \;=\; \big(\alpha\varphi(u), \psi\omega(p)\big) \;=\; (u,p)$$

□

Proof of (3.90):
Since N is free we may choose a basis $\{\, n_i \mid i \in I \,\}$ of N. And as ψ is surjective, we may choose some $m_i \in M$ such that $\psi(m_i) = n_i$ for any $i \in I$. Then we may define

$$\omega \;:\; N \to M \;:\; \sum_{i\in I} a_i n_i \mapsto \sum_{i\in I} a_i m_i$$

This is a well-defined homorphism, that satisfies $\psi\omega(n_i) = \psi(m_i) = n_i$ for any $i \in I$. As the n_i generate N this is $\psi\omega(x) = x$ and hence $\psi\omega = \mathbb{1}_N$. Thus we have property (b) in (3.89) such that by property (c) there is some isomorphism $\Phi : M \xrightarrow{\sim} L \oplus N$ that makes the diagram commute. □

Proof of (4.23):

(i) Clearly, if $b \notin \mathrm{im}(A)$, then $Ax = b$ has no solution at all, hence $\mathbb{L}(Ax = b) = \emptyset$. Conversely if $b \in \mathrm{im}(A)$ then we can pick up some $u \in R^n$ with $Au = b$. Now if $v \in \mathrm{kn}(A)$ then $A(u+v) = Au + Av = b + 0 = b$. And as v has been arbitrary, this means $u + \mathrm{kn}(A) \subseteq \mathbb{L}(Ax = b)$. Conversely consider some x with $Ax = b$, then $A(x-u) = Ax - Au = b - b = 0$ and hence $v := x - u \in \mathrm{kn}(A)$. Again, as x has been arbitrary that is $\mathbb{L}(Ax = b) \subseteq u + \mathrm{kn}(A)$.

(ii) First of all let us compute $DT^{-1} = SATT^{-1} = SA$. Further note that - due to the invertibility of S - we have the equivalence

$$b \;=\; Ax \quad\Longleftrightarrow\quad Sb \;=\; SAx \;=\; DT^{-1}x$$

Now for (a) $\Longrightarrow$ (b): let us define $z := T^{-1}x$, then $Dz = DT^{-1}x = SAx = Sb$. And $x = TT^{-1}x = Tz$ is clear, as well. Conversely for (b) $\Longrightarrow$ (a): if $x = Tz$ then $z = T^{-1}Tz = T^{-1}x$ and hence also $Sb = Dz = DT^{-1}x$ and hence $b = Ax$ by the equivalence above.

(iii) By definition $x \in \mathbb{L}(Ax = b)$ means that $Ax = b$. As we have seen in (ii) this is equivalent to $x = Tz$ and $Dz = Sb$ for some $z \in R^n$. Again this translates into $x = Tz$ and $z \in \mathbb{L}(Dx = Sb)$. And this is nothing but $x \in T\,\mathbb{L}(Dx = Sb)$.

(iv) Due to (i) we know that $\mathbb{L}(Dx = Sb)$ either is empty (if $Sb \notin \mathrm{im}(D)$) or given to be $u + \mathrm{kn}(D)$ for some special solution $Du = Sb$. Now by (iii) we have $\mathbb{L}(Ax = b) = R\mathbb{L}(Dx = Sb) = R(u + \mathrm{kn}(D))$. And since a matrix always defines an R-linear operation, this yields $\mathbb{L}(Ax = b) = Ru + R\,\mathrm{kn}(D)$.

□

Proof of (4.24):

- Since $\mathrm{im}(L) = a_1R + \cdots + a_nR = dR$ according to (2.83.(iii)) we have $b \in \mathrm{im}(L) = dR$ if and only if $d \mid b$. So $\mathbb{L} \neq \emptyset$ clearly is equivalent to $b \in \mathrm{im}(L)$ which in turn is equivalent to $d \mid b$. In

particular we may pick up some $u = (u_1, \ldots, u_n) \in R^n$ such that $L(u) = d \in dR = \mathrm{im}(L)$. That is $a_1u_1 + \cdots + a_nu_n = d$. In case $d \mid b$ there is some $\beta = b/d \in R$ satisfying $d\beta = b$, so multiplying this equation with this β yields (due to the R-linearity of L)

$$L(\beta u) \;=\; \beta L(u) \;=\; \beta d \;=\; d$$

such that $s = \beta u$ truly is a special solution to the equation $L(x) = b$. It is immediately to see that $s = (\beta u_1, \ldots, \beta u_n) \in \mathbb{L}$ is the special solution given in the claim above.

- In case $n = 1$ there is next to nothing to prove: clearly $x_1 = \beta u_1 = \beta = b/d = b/a_1$ is the special solution and this is uniquely determined since R has been assumed to bee an integral domain (even an Euclidean domain).

- In case $n = 2$ we have to prove the equality of the kernel $K := \mathrm{kn}(L)$, once this is established we know $\mathbb{L} = s + K$ from (4.23). So let us denote $\alpha_i = a_i/d$ (that is $d\alpha_i = a_i$) and consider some $x \in R^2$ of the form $x = (\alpha_2, -\alpha_1)t$ for some $t \in R$. Then it is clear that $L(x) = a_1x_1 + a_2x_2 = a_1\alpha_2 t - a_2\alpha_1 t = d\alpha_1\alpha_2 t - d\alpha_2\alpha_1 t = dt(\alpha_1\alpha_2 - \alpha_2\alpha_1) = 0$ such that $(\alpha_2, -\alpha_1)R \subseteq K$. Conversely given $x \in K$, that is $L(x) = a_1x_1 + a_2x_2 = 0$, then already $d(\alpha_1x_1 + \alpha_2x_2) = 0$. And since a_1 and $a_2 \neq 0$ we have $d = 0$ such that necessarily $\alpha_1x_1 = -\alpha_2x_2$. In particular we have $\alpha_1 \mid \alpha_2x_2$. But according to (2.58.(v)) we also know that $1 \in \gcd\{\alpha_1, \alpha_2\}$ such that by (2.64.(iv)) we get $\alpha_1 \mid x_2$, that is $x_2 = \alpha_1 t_1$ for some $t_1 \in R$. Likewise we find $x_1 = \alpha_2 t_2$ for some $t_2 \in R$. Using these equations we find $0 = \alpha_1x_1 + \alpha_2x_2 = \alpha_1\alpha_2t_2 + \alpha_2\alpha_1t_1 = \alpha_1\alpha_2(t_1 + t_2)$. Since both $\alpha_i \neq 0$ are non-zero we get $t_2 = -t_1$ such that (abbreviating $t := t_1$) we have $x_1 = \alpha_2 t$ and $x_2 = -\alpha_1 t$. This also proves the inclusion $(\alpha_2, -\alpha_1)R \subseteq K$.

- We will prove this statement by induction on the number $n \geq 2$ of variables. The case $n = 2$ has already been shown above (note that $d_1 = \gcd\{a_1\} = a_1$ and $d_2 = \gcd\{a_1, a_2\} = d$) so we continue with the induction step where $n \geq 3$. That is we regard the equation

$$a_1x_1 + \cdots + a_nx_x + a_{n+1}x_{n+1} \;=\; b$$

This equation admits a solution if and only if the greatest common divisor d_{n+1} divides b, that is iff $d_{n+1} = \gcd\{a_1, \ldots, a_n, a_{n+1}\} \mid b$. If this is untrue, then there is nothing to prove, since there is no special solution $s = b/d_{n+1}(u_{1,n+1}, \ldots, u_{n,n+1}, u_{n,n+1})$. But clearly this equation is equivalent to $a_1x_1 + \cdots + a_nx_x = b - a_{n+1}x_{n+1}$ and we know that this equation is solvable if and only if $d_n = \gcd\{a_1, \ldots, a_n\} \mid b - a_{n+1}x_{n+1}$ (note that this is equivalent to the solubility of the original equation as well). That is, there is some $z \in R$ such that we have the system of equations

$$\begin{aligned} b - a_{n+1}x_{n+1} &= zd_n \\ a_1x_1 + \cdots + a_nx_n &= zd_n \end{aligned}$$

Let us abbreviate $y = x_{n+1}$ and note that the first of these equations can be reformulated, as $a_{n+1}y + d_nz = b$. From the case $n = 2$ we already know that the solutions to this equation are given to be

$$(y, z) \;=\; \left(\frac{b}{d_{n+1}}v,\; \frac{b}{d_{n+1}}w\right) + \left(\frac{d_n}{d_{n+1}},\; -\frac{a_{n+1}}{d_{n+1}}\right) r$$

Where $r \in R$ is an arbitrary coefficient, that spans a 1-dimensional space of solutions. This is due to (2.64.(vii)) where we have seen, that $\gcd\{d_n, a_{n+1}\} = \gcd\{\gcd\{a_1, \ldots, a_n\}, a_{n+1}\} = \gcd\{a_1, \ldots, a_{n+1}\} = d_{n+1}$ and finally $v, w \in R$ are some elements satisfying $a_{n+1}v + d_n w = d_{n+1}$. Note that this can be achieved, by letting $v := u_{n+1,n+1}$ and

$$w \;:=\; \frac{a_1}{d_n}u_{1,n+1} + \cdots + \frac{a_n}{d_n}u_{n,n+1}$$

as in this case we get $a_{n+1}v + d_n w = a_{n+1}u_{n+1,n+1} + a_1 u_{1,n+1} + \cdots + a_n u_{n,n+1} = d_{n+1}$ by construction of the $u_{i,k}$. Let us finally take the coefficient to be $r_n := -r \in R$ instead, then we have

$$\begin{aligned} x_{n+1} &= \frac{b}{d_{n+1}}u_{n+1,n+1} - \frac{d_n}{d_{n+1}}r_n \\ z &= \frac{b}{d_{n+1}}w + \frac{a_{n+1}}{d_{n+1}}r_n \end{aligned}$$

We now apply the induction hypothesis to the second equation in our system $a_1x_1 + \cdots + a_n x_n = zd_n$ yielding the solutions $x \in s + \mathrm{im}(A)$ where $s \in R^n$ is a special solution, such as

$$\begin{aligned} s &= \left(\frac{zd_n}{d_n}u_{1,n}, \ldots, \frac{zd_n}{d_n}u_{n,n}\right) \\ &= (zu_{1,n}, \ldots, zu_{n,n}) \;=\; z(u_{1,n}, \ldots, u_{n,n}) \\ &= \left(\frac{b}{d_{n+1}}w + \frac{a_{n+1}}{d_{n+1}}r_n\right)(u_{1,n}, \ldots, u_{n,n}) \end{aligned}$$

So let us regard the solution $x = s + Ar$ where $x = (x_1, \ldots, x_n)$ and $r = (r_1, \ldots, r_{n-1})$, then we find that x_k ($k \in 1 \ldots n$) is given to be

$$x_k \;=\; s_k + [Ar]_k \;=\; \frac{b}{d_{n+1}}u_{k,n}w + \frac{a_{n+1}}{d_{n+1}}u_{k,n}r_n + [Ar]_k$$

Combining this result for the previous x_k ($k \in 1 \ldots n$) with our result for the current step x_{n+1} we arrive at the following matrix representation of the solution of the original equation $(x_1, \ldots, x_n, x_{n+1}) =$

$$\begin{pmatrix} bu_{1,n}w/d_{n+1} \\ \vdots \\ bu_{n,n}w/d_{n+1} \\ bu_{n+1,n+1}/d_{n+1} \end{pmatrix} + \begin{pmatrix} \boxed{A} & \begin{matrix} a_{n+1}u_{1,n}/d_{n+1} \\ \vdots \\ a_{n+1}u_{u,n}/d_{n+1} \end{matrix} \\ 0 \;\cdots\; 0 & -d_n/d_{n+1} \end{pmatrix} \begin{pmatrix} r_1 \\ \vdots \\ r_{n-1} \\ r_n \end{pmatrix}$$

It is plain to see, that this matrix is precisely the matrix given in the claim in the case of $n+1$ variables. In order to distinguish the $n \times (n-1)$ matrix A from this $(n+1) \times n$-matix, let us denote the latter by A'. Let us also denote this special solution by $s' := (bu_{1,n}w/d_{n+1}, \ldots, bu_{n,n}w/d_{n+1}, bu_{n+1,n+1}/d_{n+1})$. Then we only have to argue, that we can shift this solution s' in such a way, that we truly get $x = s + A't$ for some $t \in R^n$ and the special solution $s = b/d_{n+1}(u_{1,n+1}, \ldots, u_{n+1,n+1}) \in R^{n+1}$ given in the claim. To do this recall that

$$d_n w \;=\; (a_1u_{1,n} + \cdots + a_n u_{n,n})w \;=\; a_1u_{1,n}w + \cdots + a_n u_{n,n}w$$

Inserting this into $d_{n+1} = d_n w + a_{n+1}u_{n+1,n+1}$ we find two distinct equations for the greates common divisor d_{n+1} namely

$$\begin{aligned} d_{n+1} &= a_1u_{1,n}w + \cdots + a_nu_{n,n}w + a_{n+1}u_{n+1,n+1} \\ d_{n+1} &= a_1u_{1,n+1} + \cdots + a_nu_{n,n+1} + a_{n+1}u_{n+1,n+1} \end{aligned}$$

Subtracting these two equations we see, that $0 = a_1(u_{1,n}w - u_{1,n+1}) + \cdots + a_n(u_{n,n}w - u_{n,n+1})$. Let us now take $k = (k_1, \ldots, k_n)$ to be

$$k_j := \frac{b}{d_{n+1}}(u_{j,n}w - u_{j,n+1})$$

then by construction we see that $s' = s + (k_1, \ldots, k_n, 0)$ is the special solution we found above. But it also is clear that $a_1k_1 + \cdots + a_nk_n = 0$. That is k is a solution to the homogeneous equation $L(k) = 0$ and by induction hypothesis this means $k \in \mathrm{im}(A)$. That is $k = Aq$ for some $q \in R^{n-1}$. Let us now define $t = (t_1, \ldots, t_n) := (r_1, \ldots, r_n) + (q_1, \ldots, q_{n-1}, 0)$ then we clearly have $A't = A'r + (Aq, 0) = A'r + (k, 0)$ such that $s + A't = s + (k, 0) + A'r = s' + A'r = x$. That is we can also parametrisize the solutions x in the form $x = s + A't$ by taking to the shift $t = r + (k, 0)$ which is a bijection.

□

Proof of (4.29):

We will prove the following claim by induction on the number m of rows of the matrix A: using the Gaussian algorithm one obtains an $(m \times m)$-matrix S and an $(m \times n)$-matrix E such that E is in echelon-form. The fact, that S is a product of elementary matrices is clear from the algorithm - no other matrices are involved.

In the case $A = 0$ the algorithm already terminates at step (2), so we are left with $S = \mathbb{1}_m$ and $E = A = 0$. In this case $E = 0$ trivially is in echelon-form and $E = SA$ is clear.

So let us now assume $A \neq 0$. We first anchor the induction for $m = 1$. As $A \neq 0$ we necessarily have $s = 1 = r$ and the pivot step is skipped. Likewise the main step (5) is void, as $r + 1 \ldots m$ is empty. So again $E = A$ is in echelon-form and $E = SA$. And as $m = r$ the algorithm terminates.

Let us now assume that the claim has been proved for any matrix B with less than m rows. Then we need to show, that the claim holds true for A as well. The algorithm starts with row $r = 1$. And as $A \neq 0$ the algorithm does not terminate in (2) but targets u and s such that $u = \mu(A)$ and $\mu(\mathrm{row}_s A) = u$. In case $s \neq r = 1$ the rows 1 and s are interchanged $E = P_{r,s}A = SA$. So after step (4) we can be sure, that $\mu(\mathrm{row}_1 E) = \mu(E)$ is minimal. That is the first $u - 1$ columns of E are zero. Let us denote $p = m - 1$ and $q := n - u$ then E is of the form

$$E = \begin{pmatrix} 0 & \cdots & 0 & x_0 & x_1 & \cdots & x_q \\ 0 & \cdots & 0 & y_1 & h_{1,1} & \cdots & h_{1,q} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & y_p & h_{p,1} & \cdots & h_{p,q} \end{pmatrix}$$

That is $x = (x_0, x_1, \ldots, x_q)$ where $x_j = e_{1,u+j}$ and $y = (y_1, \ldots, y_p)$ where $y_i = e_{i+1,u}$ and $H = (h_{i,j})$ where $h_{i,j} = e_{i+1,u+j}$. Now the main step (5) is initiated. For any $i \in 2 \ldots m$ the following row-operations

are performed

$$\mathrm{row}_i E \;:=\; e_{r,u}(\mathrm{row}_i E) - e_{i,u}(\mathrm{row}_r E)$$

Specifically for the u-th column of E (that is the u-th entry of $\mathrm{row}_i E$) this is $[\mathrm{row}_i E]_u = e_{r,u}e_{i,u} - e_{i,u}e_{r,u}$ and as R is commutative this means $[\mathrm{row}_i E]_u = 0$. Hence *after* the main step the matrix E is turned into

$$E \;=\; \begin{pmatrix} 0 & \cdots & 0 & x_0 & x_1 & \cdots & x_q \\ 0 & \cdots & 0 & 0 & b_{1,1} & \cdots & b_{1,q} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & b_{p,1} & \cdots & b_{p,q} \end{pmatrix}$$

For some matrix $B = (b_{i,j})$ where $i \in 1 \ldots p = m-1$ and $j \in 1 \ldots q$. Now the Gaussian algorithm iterates with $r = 2$. As B has $m-1$ rows only, the induction hypothesis yields that the Gaussian algorithm will also transform B into echelon form. So after the algorithm terminates B is in echelon form i.e. there is some $r \in 1 \ldots m-1$ such that $\mu(\mathrm{row}_1 B) < \cdots < \mu(\mathrm{row}_r B)$ and for all $i > r$ we get $\mathrm{row}_i B = 0$. As E is in the form presented in the equation above, we have $\mu(\mathrm{row}_1 E) = u < u + \mu(\mathrm{row}_1 B) = \mu(\mathrm{row}_2 E)$ and hence

$$\mu(\mathrm{row}_1 E) \;<\; \ldots \;< \mu(\mathrm{row}_{r+1} E)$$

And for $i > r+1$ we have $\mu(\mathrm{row}_{i-1} B) = 0$ and therefore $\mu(\mathrm{row}_i E) = 0$ due to the shape of E. That is E is in echelon form, as claimed. The fact that $E = SA$ is clear, as all the operations (multiplications with elementary matrices from the left) on A are performed on S simultaneously. □

Proof of (4.33):
We have to prove that the algorithm presented in (4.34) truly comes up with some matrices P_k, L_k (where $k \in 1 \ldots n$ that satisfy the properties claimed in (4.33). To do this let us enumerate the matrix U that is used in the k-th step by U_k. Upon initialisation of the algorithm, this is $P_0 = \mathbb{1}_{n+1}$ and $U_0 = A$. In a first step we will prove that $[U_k]_{i,j} = 0$ for any $1 \leq j < k$ and any $j < i \leq n+1$ and that

$$U_k \;=\; L_k P_k U_{k-1}$$

for any $k \in 1 \ldots n$. Of course we use induction on k for that and the case $k = 0$ is void. That is we only have to regard $k \geq 1$ and work our way up. And as $U_0 = A$ the above equation already means

$$U_k \;=\; L_k P_k \ldots L_1 P_1 A$$

From this we find that U_k is invertible: A was assumed to be invertible, P_k is a permutation matrix and L_k satisfies $L_k^* \in \mathrm{tri}^1_{n+1}(F)$. Thus U_k inherits the invertibility from these matrices. First thing in the k-th step, $q(k)$ is selected, this is possible, unless $[U_{k-1}]_{i,k} = 0$ for all $i \in k \ldots n+1$. But in this case U_{k-1} had determinant 0: By Laplace expansion we see, that the determinant of U_{k-1} is

$$\det(U_{k-1}) \;=\; \left(\prod_{j=1}^{k-1} [U_{k-1}]_{j,j}\right) \cdot \det \begin{pmatrix} [U_{k-1}]_{k,k} & \cdots & [U_{k-1}]_{k,n+1} \\ \vdots & & \vdots \\ [U_{k-1}]_{n+1,k} & \cdots & [U_{k-1}]_{n+1,n+1} \end{pmatrix}$$

so the first column of this submatrix would vanish, leaving determinant 0. But we have seen that U_k has

to be invertible, a contradiction. So we find a suitable $q(k) \in k \dots n+1$. The multiplication $P_k U_k$ swaps the k and the $q(k)$-th row of U_k, which is precisely, what the algorithm does next. We also see that the algorithm assembles the matrix $L_k = \mathbb{1}_{k-1} \oplus L'_k$ where

$$L'_k \;=\; \begin{pmatrix} 1 & 0 & \dots & 0 \\ [L_k]_{k+1,k} & 1 & & \vdots \\ \vdots & & \ddots & 0 \\ [L_k]_{n+1,k} & 0 & \dots & 1 \end{pmatrix}$$

And by induction hypothesis we have $[U_k]_{i,j} = 0$ for any $1 \leq j < k$ and any $j < i \leq n+1$. That is the first $k-1$ columns U_k have a triangular matrix $T_k \in \mathrm{tri}_{k-1}(F)$ at the top, such that U_k is of the form

$$U_k \;=\; \begin{pmatrix} T_k & U''_k \\ 0 & U'_k \end{pmatrix}$$

And as $q(k) \geq k$ the transposition matrix P_k only interchanges two rows in the lower part of this matrix, but does not change its block structure. For ease of notation we therefore ignore P_k for the moment, as the algorithm continues with $P_k U_k$ in place of U_k. Take a look at

$$L_k U_k \;=\; \begin{pmatrix} \mathbb{1}_{k-1} & 0 \\ 0 & L'_k \end{pmatrix} \begin{pmatrix} T_k & U''_k \\ 0 & U'_k \end{pmatrix} \;=\; \begin{pmatrix} T_k & U''_k \\ 0 & L'_k U'_k \end{pmatrix}$$

As $\mathrm{row}_i(L_k) = e_k$ for any $i \leq k$ we find that $\mathrm{row}_i(L_k U_k) = \mathrm{row}_i(U_k)$. For $i > k$ the i-th row of L_k is $[L_k]_{i,k} e_k + e_i$ such that vector-matrix multiplication yields

$$\mathrm{row}_i(L_k U_k) \;=\; [L_k]_{i,k}\, \mathrm{row}_k(U_k) + \mathrm{row}_i(U_k)$$

That is the algorithm mimics the matrix-multiplication $L_k U_k$ here. In particular for the k-th column of $L_k U_k$ we find that our choice of $[L_k]_{i,k}$ results in $[L_k U_k]_{i,k} = 0$ for any $i > k$, as

$$[L_k]_{i,k}\, [U_k]_{k,k} + [U_k]_{i,k} \;=\; 0$$

In particular $U_{k+1} = L_k P_k U_k$ is of the same shape, as U_k before, but the upper triangular matrix $T_{k+1} \in \mathrm{tri}_k(F)$ now is of size $(k \times k)$. When we end at $k = n$ we see that $U_{n+1} = L_n P_n U_n$ is an upper triangular matrix itself. And therefore

$$U \;=\; U_{n+1} \;=\; L_n P_n U_n \;=\; \dots \;=\; L_n P_n \dots L_1 P_1 A \;\in\; \mathrm{tri}_{n+1}(F)$$

Next we want to prove that $\widehat{L}_k$ is of the same shape, as L_k. Let us call this shape *lower-k-columns-only* matrix for the moment being. This is to say L_k satifies the properties

(1) for any $i \in 1 \dots n+1$ we have $[L_k]_{i,i} = 1$

(2) for any $i < k$ we have $[L_k]_{i,k} = 0$

(3) for any $j \neq k$ and any $i \neq j$ we have $[L_k]_{i,j} = 0$

By construction L_k is a lower-k-column-only matrix and we want to prove that thereby for any $l > k$ the matrix $L'_k := P_l L_k P_l$ is lower-k-column-only matrix, too: By construction P_l is the permutation matrix of the transposition $\tau = (l\, q(l))$, where $k < l \leq q(l)$. In particular we have $\tau(j) = j$ for any $j \leq k$. Thereby P_l is self-inverse, such that $L'_k = P_l L_k P_l^{-1}$ and then (4.21.(v)) tells us that the (i,j)-th entry of L'_k is

$$[L'_k]_{i,j} \;=\; [L_k]_{\tau(i),\tau(j)}$$

So let us now check the three properties of a lower-k-column-only matrix: For any i we have $[L'_k]_{i,i} = [L_k]_{\tau(i),\tau(i)} = 1$ as needed. For any $i < k$ we have $\tau(i) = i < k = \tau(k)$ such that $[L'_k]_{i,k} = [L_k]_{i,k} = 0$ is granted, as well. If $j \neq k$ then $\tau(j) \neq \tau(k) = k$, also if $i \neq j$ then $\tau(i) \neq \tau(j)$ and as $\tau(j) \neq k$ we find $[L'_k]_{i,j} = [L_k]_{\tau(i),\tau(j)} = 0$ from property (3) of L_k. Altogether we have proved, that $P_l L_k P_l$ is a lower-k-column-only matrix again. By induction it is now clear, that

$$\widehat{L}_k \;:=\; P_n \dots P_{k+1} L_k P_{k+1} \dots P_n$$

is a lower-k-column-only matrix, too. Next note that due to $P_n^2 = \mathbb{1}_{n+1}$ down to $P_{k+1}^2 = \mathbb{1}_{n+1}$ we find that $\widehat{L}_k$ and L_k are turned into each other, by commuting with $P_n \dots P_{k+1}$

$$\widehat{L}_k P_n \dots P_{k+1} \;=\; P_n \dots P_{k+1} L_k P_{k+1} \dots P_n P_n \dots P_{k+1} \;=\; P_n \dots P_{k+1} L_k$$

Now we are good and ready to turn $\widehat{L}PA$ into U: Just replace any $\widehat{L}_k P_n \dots P_{k+1}$ by $P_n \dots P_{k+1} L_k$ beginning with $\widehat{L}_1$ and working our way to the left. If we note that $\widehat{L}_n = L_n$, we end up with

$$\begin{aligned}
\widehat{L}PA &= \widehat{L}_n \dots \widehat{L}_1 P_n \dots P_2 P_1 A \\
&= \widehat{L}_n \dots \widehat{L}_2 P_n \dots P_3 P_2 L_1 P_1 A \\
&= \widehat{L}_n \dots \widehat{L}_3 P_n \dots P_3 L_2 P_2 L_1 P_1 A \\
&= \dots \\
&= \widehat{L}_n P_n L_{n-1} \dots L_1 P_1 A \\
&= L_n P_n L_{n-1} \dots L_1 P_1 A \;=\; U
\end{aligned}$$

□

Proof of (4.54):
We start by proving (a) $\Longrightarrow$ (c): For ease of notation let us only consider the transposition $\tau = (1\,2) \in S_n$. The general transposition $\tau = (i\,j)$ only requires more effort in writing out the proof, but conveys the same idea only. By assumption on D we may expand the following term

$$\begin{aligned}
0 &= D(a_1 + a_2, a_1 + a_2, a_3, \dots, a_n) \\
&= D(a_1, a_1, a_3, \dots, a_n) + D(a_1, a_2, a_3, \dots, a_n) \\
&\quad + D(a_2, a_1, a_3, \dots, a_n) + D(a_2, a_2, a_3, \dots, a_n) \\
&= 0 + D(a_1, a_2, a_3, \dots, a_n) + D(a_2, a_1, a_3, \dots, a_n) + 0
\end{aligned}$$

and therefore $D(a_2, a_1, a_3, \dots, a_n) = -D(a_1, a_2, a_3, \dots, a_n)$ such that we have arrived at (c). And clearly this implies (b), as by (1.18.(iv)) any permutation $\sigma \in S_n$ can be decomposed into transpositions $\sigma =$

$\tau_1\tau_2\ldots\tau_s$, such that (by induction on s) it is clear that

$$\begin{aligned} D(a_{\sigma(1)}, a_{\sigma(2)}, \ldots, a_{\sigma(n)}) &= (-1)^s D(a_1, a_2, \ldots, a_n) \\ &= \operatorname{sgn}(\sigma) D(a_1, a_2, \ldots, a_n) \end{aligned}$$

Thus we have seen (c) $\implies$ (b) and the converse implication is trivial. It remains to verify (c) $\implies$ (a): For ease of notation we will regard the case $a_1 = a_2$ only. Again the general case only requires more notational effort but grants no additional insight. So let us pick up the transposition $\tau = (1\,2)$, then by assumption we have $(a_{\tau(1)}, a_{\tau(2)}, \ldots, a_{\tau(n)}) = (a_1, a_2, \ldots, a_n)$, hence

$$\begin{aligned} D(a_1, a_2, \ldots, a_n) &= D(a_{\tau(1)}, a_{\tau(2)}, \ldots, a_{\tau(n)}) \\ &= -D(a_1, a_2, \ldots, a_n) \end{aligned}$$

Altogether we found $2D(a_1, a_2, \ldots, a_n) = 0$, if now $2 \in \operatorname{NZD}(R)$ is a non-zero divisor of R this can only mean $D(a_1, a_2, \ldots, a_n) = 0$, which is precisely the claim of (a). Thus we have returned to (a) and all three statements are equivalent.

Let us now assume R is some commutative ring and $\{ a_1, a_2, \ldots, a_n \} \subseteq R^n$ are linearly dependent. That is there are some $b_i \in R$, not all zero, such that

$$\sum_{i=1}^{n} b_i\, a_i \;=\; 0$$

For ease of notation let us assume $b_1 \neq 0$. As D is linear in every argument we can use this relation to evaluate the determinant of the a_i

$$\begin{aligned} b_1\, D(a_1, a_2, \ldots, a_n) &= D(b_1 a_1, a_2, \ldots, a_n) \\ &= D\left(-\sum_{i=2}^{n} b_i a_i, a_2, \ldots, a_n \right) \\ &= \sum_{i=2}^{n} -b_i D(a_i, a_2, \ldots, a_n) \end{aligned}$$

But as D is a determinant form and $D(a_i, a_2, \ldots, a_n)$ contains a_i twice for any $i \in 2 \ldots n$ property (a) implies $D(a_i, a_2, \ldots, a_n) = 0$. Therefore $b_1\, D(a_1, a_2, \ldots, a_n) = 0$ where $b_1 \neq 0$. If R is an integral domain we may conclude $D(a_1, a_2, \ldots, a_n) = 0$. For a general commutative ring $R \neq 0$ we find $b_1 \in \operatorname{ann}(D(a_1, a_2, \ldots, a_n))$ such that

$$\{ a_1, a_2 \ldots, a_n \} \text{ linearly dependent} \quad \Longrightarrow \quad \operatorname{ann}(D(a_1, a_2, \ldots, a_n)) \;\neq\; 0$$

Negating this implication we find the implication: If $\operatorname{ann}(D(a_1, a_2, \ldots, a_n)) = 0$ then $\{ a_1, a_2 \ldots, a_n \} \subseteq R^n$ must be linearly independent. □

Proof of (4.55):

(i) Let $A^* = (a^*_{i,j})$ that is if $A = (a_{i,j})$ then the coefficients of the transpose matrix are $a^*_{i,j} = a_{j,i}$ and

hence we find

$$\det(A^*) \;=\; \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a^*_{i,\sigma(i)} \;=\; \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{\sigma(i),i}$$

Let's say $j = \sigma(i)$ then $i = \sigma^{-1}(j)$ and we can replace the index $i \in 1\dots n$ by $j \in 1\dots n$ rewriting this expression, as

$$\det(A^*) \;=\; \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) \prod_{j=1}^{n} a_{j,\sigma^{-1}(j)}$$

Also note that $S_n \to S_n : \sigma \mapsto \sigma^{-1}$ is bijective and that $\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma)$, such that we may once again rewrite

$$\begin{aligned}\det(A^*) \;&=\; \sum_{\sigma^{-1}\in S_n} \operatorname{sgn}(\sigma^{-1}) \prod_{j=1}^{n} a_{j,\sigma^{-1}(j)} \\ &=\; \sum_{\pi\in S_n} \operatorname{sgn}(\pi) \prod_{j=1}^{n} a_{j,\pi(j)} \;=\; \det(A)\end{aligned}$$

(ii) In a first step we will prove $D(\mathbb{1}_n) = 1$, the proof multiplicative property will be postponed until after we have also proved (iv). Now clearly we have $\operatorname{col}_j(\mathbb{1}_n) = e_j$ where e_j is the Euclidean basis vector $e_j = (\delta_{i,j}) \in R^n$. Therefore

$$\det(\mathbb{1}_n) \;=\; \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma)\, \delta_{1,\sigma(1)}\delta_{2,\sigma(2)} \dots \delta_{n,\sigma(n)}$$

Thus all the summands vanish, except for the one permutation σ that satisfies $\sigma(1) = 1$, $\sigma(2) = 2$ and so on until $\sigma(n) = n$. That is $\sigma = \mathbb{1}$ is the identity, which is of signum $\operatorname{sgn}(\mathbb{1}) = 1$. Hence $\det(\mathbb{1}_n) = 1$.

(iii) Let us first prove, that the determinant is a multi-linear form. To do this we fix any permutation $\sigma \in S_n$ and define $D_\sigma : (R^n)^n \to R$ by

$$D_\sigma(a_1, a_2, \dots, a_j) \;:=\; a_{\sigma^{-1}(1),1} a_{\sigma^{-1}(2),2} \dots a_{\sigma^{-1}(n),n}$$

where $a_j = (a_{1,j}, a_{2,j}, \dots, a_{n,j}) \in R^n$ as usual. That is D_σ picks one entry from every a_j and multiplies all these. In particular D_σ is linear in every argument, i.e. it is multi-linear. On the other hand the determinant is just

$$\det \;=\; \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma)\, D_\sigma$$

an R-linear combination of these multi-linear maps - also refer to remark (4.53.(ii)) for more details on this. And thereby det clearly is multi-linear itself.

Next we will prove that $\det(A) = 0$ whenever A has two identical columns. For ease of notation let us assume $a_1 = a_2$, the general case uses precisely the same idea. Let $\tau := (1\,2) \in S_n$ be the transposition on 1 and 2, then clearly $\tau^{-1} = (2\,1) = \tau$. For a start, note that $a_1 = a_2$ in particular

means $a_{\sigma^{-1}(1),1} = a_{\sigma^{-1}(1),2}$ and likewise $a_{\sigma^{-1}(2),1} = a_{\sigma^{-1}(2),2}$. Therefore we get

$$\begin{aligned} D_\sigma(a_1, a_2, a_3, \ldots, a_n) &= a_{\sigma^{-1}(1),1} a_{\sigma^{-1}(2),2} \prod_{j=3}^{n} a_{\sigma^{-1}(j),j} \\ &= a_{\sigma^{-1}(1),2} a_{\sigma^{-1}(2),1} \prod_{j=3}^{n} a_{\sigma^{-1}(j),j} \\ &= a_{\sigma^{-1}\tau(2),2} a_{\sigma^{-1}\tau(1),1} \prod_{j=3}^{n} a_{\sigma^{-1}\tau(j),j} \\ &= a_{\sigma^{-1}\tau(1),1} a_{\sigma^{-1}\tau(2),2} \prod_{j=3}^{n} a_{\sigma^{-1}\tau(j),j} \\ &= D_{\tau\sigma}(a_1, a_2, a_3, \ldots, a_n) \end{aligned}$$

The latter, since $(\tau\sigma)^{-1} = \sigma^{-1}\tau^{-1} = \sigma^{-1}\tau$. That is, we have seen, that in case $a_1 = a_2$ we have the equality

$$D_\sigma(a_1, a_2, \ldots, a_n) = D_{\tau\sigma}(a_1, a_2, \ldots, a_n)$$

Recall that $A_n = \{\, \sigma \in S_n \mid \mathrm{sgn}(\sigma) = 1 \,\}$ and let us also denote $B_n = \{\, \pi \in S_n \mid \mathrm{sgn}(\pi) = -1 \,\}$ here. Then it is clear, that S_n is the disjoint union $S_n = A_n \cup B_n$ and hence we have

$$\det = \sum_{\sigma \in A_n} \mathrm{sgn}(\sigma)\, D_\sigma + \sum_{\pi \in B_n} \mathrm{sgn}(\pi)\, D_\pi$$

But clearly $S_n \longleftrightarrow S_n : \sigma \mapsto \tau\sigma$ is a bijection (this is true in any group). In this case however we have $\mathrm{sgn}(\tau\sigma) = -\mathrm{sgn}(\sigma)$, such that under this bijection A_n and B_n are interchanged: That is $\tau A_n = B_n$ and $\tau B_n = A_n$. Therefore $\pi \in B_n = \tau A_n$ means $\pi = \tau\sigma$ for some $\sigma \in A_n$. That is we may rewrite the sum over $\pi \in B_n$ in terms of

$$\det = \sum_{\sigma \in A_n} \mathrm{sgn}(\sigma)\, D_\sigma + \sum_{\sigma \in A_n} \mathrm{sgn}(\tau\sigma)\, D_{\tau\sigma}$$

Using $\mathrm{sgn}(\tau\sigma) = -\mathrm{sgn}(\sigma)$ and rejoining the sum we see, that the determinant can be evaluated by using even permutations only

$$\det = \sum_{\sigma \in A_n} \mathrm{sgn}(\sigma) \Big(D_\sigma - D_{\tau\sigma} \Big)$$

However, if $a_1 = a_2$ then we have argued above, that for this particular $A = (a_1, a_2, \ldots, a_n)$ we have $D_\sigma(A) = D_{\tau\sigma}(A)$ and therefore we find, that the determinant truly vanishes

$$\det(A) = \sum_{\sigma \in A_n} \mathrm{sgn}(\sigma) \Big(D_\sigma(A) - D_{\tau\sigma}(A) \Big) = \sum_{\sigma \in A_n} \mathrm{sgn}(\sigma) \cdot 0 = 0$$

(iv) Consider any n-tuples $a_j = (a_{i,j}) \in R^n$ where $j \in 1 \ldots n$ as well. If $e_i = (\delta_{i,j}) \in R^n$ denotes i-th the Euclidean base vector of size n then it is plain to see, that

$$a_j = \sum_{i=1}^{n} a_{i,j} e_i \in R^n$$

As we will do this with any a_j let use a separate index $\alpha(j)$ instead of i. Using this the above identity will now be written as

$$a_j \;=\; \sum_{\alpha(j)=1}^{n} a_{\alpha(j),j} e_{\alpha(j)}$$

By assumption D is a determinant form, in particular it is linear in each argument. Therefore we may expand all these a_j to find the following expression

$$\begin{aligned} D(a_1,\ldots,a_n) &= D\left(\sum_{\alpha(1)=1}^{n} a_{\alpha(1),1} e_{\alpha(1)},\ldots,\sum_{\alpha(n)=1}^{n} a_{\alpha(n),n} e_{\alpha(n)}\right) \\ &= \sum_{\alpha(1)=1}^{n}\cdots\sum_{\alpha(n)=1}^{n} a_{\alpha(1),1}\ldots a_{\alpha(n),n} D\left(e_{\alpha(1)},\ldots,e_{\alpha(n)}\right) \end{aligned}$$

If $\alpha(i)=\alpha(j)$ for some $i\neq j\in 1\ldots n$, then clearly $e_{\alpha(i)}=e_{\alpha(j)}$ such that by assumption (D is a determinant form) we then find $D(e_{\alpha(1)},\ldots,e_{\alpha(n)})=0$. Therefore only summands remain in which $i\neq j \implies \alpha(i)\neq\alpha(j)$, that is in which $\alpha\in S_n$ is a permutation

$$D(a_1,\ldots,a_n) \;=\; \sum_{\alpha\in S_n} a_{\alpha(1),1}\ldots a_{\alpha(n),n} D\left(e_{\alpha(1)},\ldots,e_{\alpha(n)}\right)$$

But since D is a determinant form, we have already seen in (4.54) that D also is alternating. In particular for any $\alpha\in S_n$ we find

$$D\left(e_{\alpha(1)},\ldots,e_{\alpha(n)}\right) \;=\; \operatorname{sgn}(\alpha) D\left(e_1,\ldots,e_n\right) \;=\; \operatorname{sgn}(\alpha) D(\mathbb{1}_n)$$

Altogether we have arrived at the following identity

$$\begin{aligned} D(a_1,\ldots,a_n) &= \sum_{\alpha\in S_n} a_{\alpha(1),1}\ldots a_{\alpha(n),n}\operatorname{sgn}(\alpha) D(\mathbb{1}_n) \\ &= D(\mathbb{1}_n)\sum_{\alpha\in S_n}\operatorname{sgn}(\alpha)\, a_{\alpha(1),1}\ldots a_{\alpha(n),n} \end{aligned}$$

Once again we use the bijection $S_n \longleftrightarrow S_n : \alpha\mapsto\alpha^{-1}$ to sum over $\sigma := \alpha^{-1}$ instead. As $\operatorname{sgn}(\sigma)=\operatorname{sgn}(\alpha^{-1})=\operatorname{sgn}(\alpha)$ we finally see that this sum turns into precisely the expression we are aiming at

$$\begin{aligned} D(a_1,\ldots,a_n) &= D(\mathbb{1}_n)\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)\, a_{\sigma^{-1}(1),1}\ldots a_{\sigma^{-1}(n),n} \\ &= D(\mathbb{1}_n)\cdot\det(a_1,\ldots,a_n) \end{aligned}$$

(ii) It remains to prove the homomorphism property of the determinant: To see this define $D:\operatorname{mat}_n(R)\to R$ by $D(B):=\det(AB)$. By definition of the multiplication of matrices we have $\operatorname{col}_i(AB)=A\operatorname{col}_i(B)$. That is (for any $b_1, b_2,\ldots,b_n\in R^n$) we have

$$D(b_1,b_2,\ldots,b_n) \;=\; \det(Ab_1,\, Ab_2,\,\ldots,\, Ab_n)$$

and hence all the maps $R^n\to R : b_k\mapsto D(b_1,b_2,\ldots,b_n)$ are just compositions of the linear maps

$R^n \to R^n : b_k \mapsto Ab_k$ and $R^n \to R : c_k \mapsto \det(c_1, c_2, \ldots, c_n)$ and therefore are linear themselves. In other words D is multi-linear. But also, whenever $b_j = b_k$ for some $j \neq k$, then $Ab_j = Ab_k$ such that $\det(Ab_1, Ab_2, \ldots, Ab_n) = 0$, which means that D even is a determinant form. Now by (iv) we get

$$\det(AB) \;=\; D(B) \;=\; D(\mathbb{1}_n) \cdot \det(B) \;=\; \det(A) \cdot \det(B)$$

(v) In a first step we will prove the Laplace expansion theorem by expanding along the bottom row. That is we start with a size $(n+1) \times (n+1)$ matrix $A = (a_{i,j}) \in \mathrm{mat}_{n+1}(R)$ and choose $p = n+1$. Then clearly

$$A_q \;:=\; A_{n+1,q} \;=\; \begin{pmatrix} a_{1,1} & a_{1,2} & \ldots & a_{1,q-1} & a_{1,q+1} & \ldots & a_{1,n+1} \\ a_{2,1} & a_{2,2} & \ldots & a_{2,q-1} & a_{2,q+1} & \ldots & a_{2,n+1} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ a_{n,1} & a_{n,2} & \ldots & a_{n,q-1} & a_{n,q+1} & \ldots & a_{n,n+1} \end{pmatrix}$$

We identify S_n with $\{\, \varrho \in of S_{n+1} S_{n+1} \mid \varrho(n+1) = n+1 \,\}$, a subgroup of S_{n+1}. Then by (1.12.(ii)) we know that S_{n+1} is the disjoint union

$$S_{n+1} \;=\; \bigcup_{q=1}^{n+1} \tau_q S_n$$

where τ_q is the transposition $\tau_q = (q \;\; n+1) \in S_{n+1}$. Thereby we can split the sum in the determinant of A into $n+1$ separate parts

$$\begin{aligned} \det(A) \;&=\; \sum_{\sigma \in S_{n+1}} \mathrm{sgn}(\sigma) \prod_{i=1}^{n+1} a_{i,\sigma(i)} \\ &=\; \sum_{q=1}^{n+1} \sum_{\varrho \in S_n} \mathrm{sgn}(\tau_q \varrho) \prod_{i=1}^{n+1} a_{i,\tau_q\varrho(i)} \end{aligned}$$

If $q = n+1$ then $\tau_q = \mathbb{1}$ and hence $\mathrm{sgn}(\tau_q\varrho) = \mathrm{sgn}(\varrho)$ if $q = n+1$ and $\mathrm{sgn}(\tau_q\varrho) = -\mathrm{sgn}(\varrho)$ in any other case. Also $\tau_q\varrho(i) = q$ if $i = n+1$, likewise $\tau_q\varrho(i) = n+1$ if $\varrho(i) = q$ and $\tau_q\varrho(i) = \varrho(i)$ in any other case. Therefore

$$\begin{aligned} \det(A) \;&=\; \sum_{\varrho \in S_n} \mathrm{sgn}(\varrho) \left(\prod_{i=1}^{n} a_{i,\varrho(i)} \right) a_{n+1,n+1} \\ &\quad - \sum_{q=1}^{n} \sum_{\varrho \in S_n} \mathrm{sgn}(\varrho) \left(\prod_{i=1}^{n} a_{i,\tau_q\varrho(i)} \right) a_{n+1,q} \end{aligned}$$

In the first part of this expression we clearly see the determinant of A_{n+1}. In the second part we see the determinant of the matrix A_{n+1} in which the q-th column has been replaced by the $(n+1)$-st colums

$$\sum_{\varrho \in S_n} \mathrm{sgn}(\varrho) \prod_{i=1}^{n} a_{i,\tau_q\varrho(i)}$$

$$= \det \begin{pmatrix} a_{1,1} & \dots & a_{1,q-1} & a_{1,n+1} & a_{1,q+1} & \dots & a_{1,n} \\ a_{2,1} & \dots & a_{2,q-1} & a_{2,n+1} & a_{2,q+1} & \dots & a_{2,n} \\ \vdots & & \vdots & \vdots & & \vdots & \\ a_{n,1} & \dots & a_{n,q-1} & a_{n,n+1} & a_{n,q+1} & \dots & a_{n,n} \end{pmatrix}$$

This matrix can be obtained from A_q by moving the last column of A_q one step up front $n-q$ times. As det is a determinant form and hence alternating, this means

$$\sum_{\varrho \in S_n} \operatorname{sgn}(\varrho) \prod_{i=1}^{n} a_{i,\tau_q \varrho(i)} \quad = \quad (-1)^{n-q} \det(A_q)$$

Altogether we have found the following expression for the determinant

$$\det(A) \quad = \quad \det(A_{n+1}) a_{n+1,n+1} - \sum_{q=1}^{n} (-1)^{n-q} \det(A_q) a_{n+1,q}$$

Since $(-1)^{2q} = 1$ we find $-(-1)^{n-q} = (-1)^{n-q+1}(-1)^{2q} = (-1)^{n+1+q}$ and if we recall $p = n+1$ this is $-(-1)^{n-q} = (-1)^{p+q}$. Therefore this identity can finally be written as

$$\begin{aligned} \det(A) &= a_{n+1,n+1} \det(A_{n+1}) + \sum_{q=1}^{n} (-1)^{p+q} a_{n+1,q} \det(A_q) \\ &= \sum_{q=1}^{n+1} (-1)^{p+q} a_{n+1,q} \det(A_q) \end{aligned}$$

That is we have proved the Laplace expansion theorem in case $p = n+1$. i.e. when expanding along the bottom row of A. For arbitrary $p \in 1 \dots n+1$ consider the matrix

$$B \quad := \quad \begin{pmatrix} \text{---} & \operatorname{row}_1(A) & \text{---} \\ & \vdots & \\ \text{---} & \operatorname{row}_{p-1}(A) & \text{---} \\ \text{---} & \operatorname{row}_{p+1}(A) & \text{---} \\ & \vdots & \\ \text{---} & \operatorname{row}_{n+1}(A) & \text{---} \\ \text{---} & \operatorname{row}_p(A) & \text{---} \end{pmatrix}$$

This matrix is obtained from A by moving the p-th row of A down one step, $n+1-p$ many times. Again - since det is alternating

$$\det(B) \quad = \quad (-1)^{n+1-p} \det(A)$$

On the other hand, we may expand B along the bottom row already. Doing so we find the following identity [note that $b_{n+1,q} = a_{p,q}$]

$$\det(B) \quad = \quad \sum_{q=1}^{n+1} (-1)^{n+1+q} a_{p,q} \det(B_q)$$

Thereby we also have $B_q = A_{p,q}$ by construction, such that joining these two equalities we find the following identity

$$(-1)^{n+1-p}\det(A) \;=\; \sum_{q=1}^{n+1}(-1)^{n+1+q}a_{p,q}\det(A_{p,q})$$

By multiplying with $(-1)^{n+1-p}$ and using $(-1)^{2n+2} = 1$ this is precisely the formula in the Laplace expansion theorem. So it oly remains to prove, that this formula also holds true when expanding along the q-th column of A. But this third step can be easily done by expanding the transpose A^* along the q-th row. Doing this we get

$$\det(A^*) \;=\; \sum_{p=1}^{n+1}(-1)^{q+p}a^*_{q,p}\det(A^*_{q,p})$$

By construction it is clear, that $(A^*)_{q,p} = (A_{p,q})^*$ and due to (i) these two matrices share the same determinant. The same is true for A and A^* of course, so rewriting $a^*_{q,p} = a_{p,q}$ we finally found the formula for expanding along a column, as well:

$$\det(A) \;=\; \sum_{p=1}^{n+1}(-1)^{p+q}a_{p,q}\det(A_{p,q})$$

(vi) By definition the determinant is just a combination of sums and products. Since α is a homomorphism of rings we have $\alpha(1_R) = 1_S$ such that for any permutation $\sigma \in S_n$ we have $\alpha(\mathrm{sgn}(\sigma)) = \mathrm{sgn}(\sigma) \in S$. And thereby we may compute

$$\begin{aligned}
\det\big(\alpha(A)\big) &= \sum_{\sigma\in S_n}\mathrm{sgn}(\sigma)\prod_{i=1}^{n}\alpha(a_{i,\sigma(i)}) \\
&= \sum_{\sigma\in S_n}\alpha(\mathrm{sgn}(\sigma))\alpha\left(\prod_{i=1}^{n}a_{i,\sigma(i)}\right) \\
&= \alpha\left(\sum_{\sigma\in S_n}\mathrm{sgn}(\sigma)\prod_{i=1}^{n}a_{i,\sigma(i)}\right) \\
&= \alpha\big(\det(A)\big)
\end{aligned}$$

□

Proof of (4.58):

(i) Let us abbreviate the block matrix by X and denote its entries by $x_{i,j}$ where $i, j \in 1\ldots(m+n)$, that is

$$X \;:=\; (x_{i,j}) \;=\; \begin{pmatrix} A & C \\ 0 & B \end{pmatrix}$$

Let us also introduce $I := 1\ldots m$ and $J := (m+1)\ldots(m+n)$ and let us finally identify S_m and S_n with certain subgroups of S_{m+n}:

$$S_m \;\cong_{\mathrm{g}}\; S'_m \;:=\; \{\,\varrho \in S_{m+n} \mid \forall\, j \in J : \varrho(j) = j\,\}$$

$$S_n \;\cong_{\mathrm{g}}\; S'_n \;:=\; \{\,\sigma \in S_{m+n} \mid \forall\, i \in I : \sigma(i) = i\,\}$$

If $\varrho \in S'_m$ and $\sigma \in S'_n$ then clearly $\mathrm{dom}(\varrho) \cap \mathrm{dom}(\sigma) \subseteq I \cap J = \emptyset$ and hence we have $\varrho\sigma = \sigma\varrho$. Now let us have a look at the determinant

$$\det(X) \;=\; \sum_{\pi \in S_{m+n}} \mathrm{sgn}(\pi) \prod_{i=1}^{m+n} x_{i,\pi(i)}$$

However, by the design of X, we have $x_{i,j} = 0$ whenever $i > m$ and $j \leq m$. That is $i \in J$ and $j \in I \implies x_{i,j} = 0$. In particular we find

$$\exists\, i \in J \,:\, \pi(i) \in I \quad\Longrightarrow\quad \prod_{i=1}^{m+n} x_{i,\pi(i)} \;=\; 0$$

Therefore the product vanishes unless $\pi(J) \subseteq J$ and since π is bijective this also implies $\pi(I) \subseteq I$. For such a π let us define $\varrho \in S'_m$ by $\varrho(i) := \pi(i)$ and $\varrho(j) := j$ where $i \in I$ and $j \in J$ respectively. Likewise define $\sigma \in S'_n$ by letting $\sigma(i) := i$ and $\sigma(j) := \pi(j)$. Then it is clear, that $\pi = \varrho\sigma$ such that

$$\begin{aligned}
\mathrm{sgn}(\pi) \prod_{i=1}^{m+n} x_{i,\pi(i)} &= \mathrm{sgn}(\varrho\sigma) \prod_{i=1}^{m} x_{i,\varrho(i)} \prod_{j=m+1}^{m+n} x_{i,\sigma(j)} \\
&= \left(\mathrm{sgn}(\varrho) \prod_{i=1}^{m} x_{i,\varrho(i)}\right)\left(\mathrm{sgn}(\sigma) \prod_{j=m+1}^{m+n} x_{j,\sigma(j)}\right) \\
&= \left(\mathrm{sgn}(\varrho) \prod_{i=1}^{m} a_{i,\varrho(i)}\right)\left(\mathrm{sgn}(\sigma) \prod_{j=1}^{n} b_{j,\sigma(j)}\right)
\end{aligned}$$

In the last step we used the identification $S_m = S'_m$ or - if we wanted to be formal - we would have to introduce $\sigma(j) := \sigma'(j+m) - m$ for this. As the product vanishes for all π that cannot be written in this form $\pi = \varrho\sigma$ the sum in truth only runs over

$$\begin{aligned}
\det(C) &= \sum_{\varrho \in S'_m} \sum_{\sigma \in S'_n} \mathrm{sgn}(\pi) \prod_{i=1}^{m+n} x_{i,\pi(i)} \\
&= \sum_{\varrho \in S'_m} \sum_{\sigma \in S'_n} \left(\mathrm{sgn}(\varrho) \prod_{i=1}^{m} a_{i,\varrho(i)}\right)\left(\mathrm{sgn}(\sigma) \prod_{j=1}^{n} b_{j,\sigma(j)}\right) \\
&= \left(\sum_{\varrho \in S'_m} \mathrm{sgn}(\varrho) \prod_{i=1}^{m} a_{i,\varrho(i)}\right)\left(\sum_{\sigma \in S'_n} \mathrm{sgn}(\sigma) \prod_{j=1}^{n} b_{j,\sigma(j)}\right) \\
&= \Big(\det(A)\Big)\Big(\det(B)\Big)
\end{aligned}$$

(ii) This is just a special case of (i) where $C = 0 \in \mathrm{mat}_{m,n}(R)$. So there really is nothing left to prove.

(iii) We will prove the statement for lower triangular matrices T. Upper triangular matrices are included, as they are the transpose of a lower triangular matrix. Recall that the determinant has been defined, as

$$\det(T) \;=\; \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} t_{i,\sigma(i)}$$

Consider any permutation $\sigma \neq \mathbb{1}$ and let $i := \min\{\, j \in 1 \ldots n \mid \sigma(j) \neq j \,\}$. As i is minimal this

means $\sigma(h) = h$ for all $h < i$. If we had $\sigma(i) < i$ then for $h := \sigma(i)$ we had $\sigma(h) = h = \sigma(i)$ in contradiction to σ being injective. Hence we necessarily have $i < \sigma(i)$. But since T is a lower triangular matrix this means $t_{i,\sigma(i)} = 0$ and hence the entire product $\prod_i t_{i,\sigma(i)}$ vanishes. The only permutation which avoids this is $\sigma = \mathbb{1}$ with $\mathrm{sgn}(\mathbb{1}) = 1$. Hence the entire determinant boils down to

$$\det(T) \;=\; \sum_{\sigma=\mathbb{1}} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} t_{i,\sigma(i)} \;=\; \prod_{i=1}^{n} t_{i,i}$$

□

Proof of (4.63):

(iv) Consider any $p, q \in 1 \ldots n$; if we scratch the p-th row and q-th column of A and transpose the rest, we obtain the same matrix, as if we had started with A^* and had scratched the q-th row and p-th column. Therefore we have

$$(A_{p,q})^* \;=\; (A^*)_{q,p}$$

Let now $c_{p,q}$ be the (p,q)-th entry of the cofactor matrix of A, that is $c_{p,q} = (-1)^{p+q}\det(A_{p,q})$. Likewise let $c^*_{q,p}$ be the (q,p)-th entry of the cofactor matrix of A^* that is $c^*_{q,p} = (-1)^{p+q}\det((A^*)_{q,p})$. As transposition does not change the determinant according to (4.55.(i)) we may compute

$$\begin{aligned} c^*_{q,p} &= (-1)^{p+q}\det\left((A^*)_{q,p}\right) \\ &= (-1)^{p+q}\det\left((A_{p,q})^*\right) \\ &= (-1)^{p+q}\det\left(A_{p,q}\right) \\ &= c_{p,q} \end{aligned}$$

That is the cofactor matrix $\mathrm{cof}(A^*)$ of the transpose is just the transpose matrix $\mathrm{cof}(A)^*$ of the cofactor matrix of A. And if this is true for the cofactor matrices, then it remains true for their transposes, the adjungate matrices.

(i) It might come as a surprise, but the proof of this theorem is purely computational. To begin with, fix $q \in 1 \ldots n$ and for $p \in 1 \ldots n$ let

$$c_p \;:=\; (-1)^{p+q}\det(A_{p,q})$$

Then by the Laplace expansion theorem (4.55.(v)) (expanding along the q-th column) it is clear that the c_p satisfy

$$\sum_{p=1}^{n} c_q a_{p,q} \;=\; \sum_{p=1}^{n} (-1)^{p+q} a_{p,q}\det(A_{p,q}) \;=\; \det(A)$$

On the other hand if $k \in 1 \ldots n$ with $k \neq q$ then by the same theorem we see that we expand the determinant along the q-th column of another matrix, namely

$$\sum_{p=1}^{n} c_q a_{p,k} \;=\; \det\begin{pmatrix} | & & | & | & | & & | \\ a_1 & \cdots & a_{q-1} & a_k & a_{q+1} & \cdots & a_n \\ | & & | & | & | & & | \end{pmatrix}$$

But since $k \in (1 \ldots q-1) \cup (q+1 \ldots n)$ this matrix contains the column a_k *twice*. That is the

determinant has to be zero, such that

$$\sum_{p=1}^{n} c_q a_{p,k} \;=\; 0 \quad \text{for } k \neq q$$

Let us now write out what the SLE $Ax = b$ means, explicitly. In fact this is precisely how the matrix multiplication has been defined

$$\begin{aligned} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n &= b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n &= b_2 \\ \vdots & \quad \vdots \\ a_{n,1}x_1 + a_{n,2}x_2 + \cdots + a_{n,n}x_n &= b_n \end{aligned}$$

We now multiply the first equation by c_1, the second equation by c_2 and do on until the last equation is multiplied by c_n

$$\begin{aligned} c_1a_{1,1}x_1 + c_1a_{1,2}x_2 + \cdots + c_1a_{1,n}x_n &= c_1b_1 \\ c_2a_{2,1}x_1 + c_2a_{2,2}x_2 + \cdots + c_2a_{2,n}x_n &= c_2b_2 \\ \vdots & \quad \vdots \\ c_na_{n,1}x_1 + c_na_{n,2}x_2 + \cdots + c_na_{n,n}x_n &= c_nb_n \end{aligned}$$

In a final step we sum up all these new equations, doing this we find the next equation, which is

$$\left(\sum_{p=1}^{n} c_p a_{p,1}\right) x_1 + \cdots + \left(\sum_{p=1}^{n} c_p a_{p,n}\right) x_n \;=\; \sum_{p=1}^{n} c_p b_p$$

As we have seen the sums over $c_p a_{p,k}$ vanish unless $k = q$. But in case $k = q$ the sum turns out to be $\det(A)$. That is in truth only

$$\det(A)\, x_q \;=\; \sum_{p=1}^{n} c_p b_p$$

But looking at the right hand side of this equation, we see, that this sum is just another expansion of another determinant along the q-th column, this time it is

$$\sum_{p=1}^{n} c_q b_k \;=\; \det\begin{pmatrix} | & & | & | & | & & | \\ a_1 & \cdots & a_{q-1} & b & a_{q+1} & \cdots & a_n \\ | & & | & | & | & & | \end{pmatrix}$$

(iii) Note that the coefficient c_p defined in (i) is just the (p,q)-th coefficient $c_{p,q} = (-1)^{p+q}\det(A_{p,q})$ of the cofactor matrix of A. So we have just shown in (i) that for any $k \in 1 \ldots n$ we find

$$\sum_{p=1}^{n} c_{p,q}\, a_{p,k} \;=\; \det(A) \cdot \delta_{k,q}$$

Let $a^{\#}_{p,q}$ be the (p,q)-th entry of the adjugate matrix $A^{\#}$ that is $a^{\#}_{q,p} = c_{p,q}$. Then the above equation

turns into

$$\sum_{p=1}^{n} a^{\#}_{q,p}\, a_{p,k} \;=\; \det(A)\cdot\delta_{k,q}$$

Note that the sum on the left hand side is just the scalar product of the q-th row of $A^{\#}$ with the k-th column a_k of A. But this is precisely the (q,k)-th entry of the product matrix $A^{\#}A$

$$\left[A^{\#}A\right]_{q,k} \;=\; \langle \mathrm{row}_q(A^{\#}, \mathrm{col}_k(A)\rangle \;=\; \det(A)\cdot\delta_{k,q}$$

And as this holds true for any k, $q \in 1\ldots n$ this is precisely $A^{\#}A = \det(A)\mathbb{1}_n$ in terms of coefficients. It remains to prove the other ordering $AA^{\#} = \det(A)\mathbb{1}_n$. But this can be done by using (iv) and going to the transpose matrix

$$\begin{aligned}
\left(AA^{\#}\right)^{*} &= \left(A^{\#}\right)^{*} A^{*} \;=\; \left(A^{*}\right)^{\#} A^{*} \\
&= \det\left(A^{*}\right)\mathbb{1}_n \;=\; \det(A)\mathbb{1}_n \\
\Longrightarrow\; AA^{\#} &= \left(\det(A)\mathbb{1}_n\right)^{*} \;=\; \det(A)\mathbb{1}_n
\end{aligned}$$

(ii) If A is invertible then by the homomorphism property of the determinant (4.55.(ii)) we see, that $\det(A)$ is invertible in R, as

$$1 \;=\; \det(\mathbb{1}_n) \;=\; \det(A^{-1}A) \;=\; \det(A^{-1})\cdot\det(A)$$

and from this we also see $\det(A^{-1}) = \det(A)^{-1}$ (as R is commutative). If conversely $\det(A) \in R^{*}$ is invertible, then we may define the matrix $B := \det(A)^{-1}\, A^{\#}$. Then from (iii) we see, that B is the inverse of A

$$\begin{aligned}
BA &= \det(A)^{-1}\, A^{\#}A \;=\; \det(A)^{-1}\det(A)\,\mathbb{1}_n \;=\; \mathbb{1}_n \\
AB &= A\det(A)^{-1}\, A^{\#} \;=\; \det(A)^{-1}\, AA^{\#} \\
&= \det(A)^{-1}\det(A)\,\mathbb{1}_n \;=\; \mathbb{1}_n
\end{aligned}$$

(v) If A is invertible (as a matrix), then so is $\det(A)$ (as a scalar) due to (ii). Then using (iii) it is easy to see, that $B := \det(A)^{-1}A$ is the inverse of $A^{\#}$ since

$$\begin{aligned}
BA^{\#} &= \det(A)^{-1}AA^{\#} \;=\; \det(A)^{-1}\det(A)\mathbb{1}_n \;=\; \mathbb{1}_n \\
A^{\#}B &= A^{\#}\det(A)^{-1}A \;=\; \det(A)^{-1}A^{\#}A \\
&= \det(A)^{-1}\det(A)\mathbb{1}_n \;=\mathbb{1}_n
\end{aligned}$$

That is we have proved $(A^{\#})^{-1} = B = \det(A)^{-1}A$ in case A is invertible. But then we may use (iii) on A^{-1} as well, to also obtain the identity $(A^{-1})^{\#}A^{-1} = \det(A^{-1})\mathbb{1}_n$. Multiplying this equation by A from the right we get

$$\left(A^{-1}\right)^{\#} \;=\; \det(A^{-1})A \;=\; \det(A)^{-1}A \;=\; \left(A^{\#}\right)^{-1}$$

On the other hand, since the determinant is linear in each of it's n arguments we get $\det(A^{\#}) =$

$\det(A)^{n-1}$ by dividing one $\det(A)$ from the following equation

$$\det(A)^n \;=\; \det(\det(A)\mathbb{1}_n) \;=\; \det(A^{\#}A) \;=\; \det(A^{\#})\cdot\det(A)$$

□

Proof of (4.65):

(i) We have already seen (a) $\iff$ (b) in (4.63.(ii)), next we will also prove (b) $\iff$ (e): To be invertible means that for any $b \in R^n$ there is precisely one $x = (x_1, x_2, \ldots, x_n) \in R^n$ such that $Ax = b$ (namely $x = A^{-1}b$). But this is $b = Ax = x_1c_1 + x_2c_2 + \cdots + x_nc_n$ which is just what we required for $\{\, c_1, c_2, \ldots, c_n \,\}$ being a basis.

Since $\det(A^*) = \det(A)$ and the columns of A^* are just the rows of A we also find that (f) is equivalent to $\det(A^*) \in R^*$ which is again equivalent to (b). Thus we also have (f) $\iff$ (b).

The implication (b) $\implies$ (c) and (d) is clear, so it remains to prove the converse implication only. If $AB = \mathbb{1}_n$ then due to (4.55.(ii)) we have $1 = \det(\mathbb{1}_n) = \det(AB) = \det(A)\cdot\det(B)$. As R is commutative this means $\det(A) \in R^*$ which is (a) and hence (b). The same argument also proves (d) $\implies$ (b) so we are done now.

(ii) By definition $\mathrm{kn}(A) \neq 0$ means, there is some $x = (x_1, x_2, \ldots, x_n) \in R^n$ such that $x \neq 0$ but $Ax = x_1c_1 + x_2c_2 + \cdots + x_nc_n = 0$. But this is just the R-linear dependency of $\{\, c_1, c_2, \ldots, c_n \,\}$. Thus we have finished (b) $\iff$ (c).

Next we will prove the equivalence of (a) and (c). Let us suppose (c) was untrue, i.e. there is some $x = (x_1, x_2, \ldots, x_n) \in R^n$ with $x \neq 0$ and $x_1c_1 + x_2c_2 + \cdots + x_nc_n = 0$. For ease of notation let us assume $x_1 \neq 0$, then - as the determinant is linear in every argument - we see

$$\begin{aligned} 0 \;&=\; \det(0, c_2, \ldots, c_n) \\ &=\; \det\left(\sum_{i=1}^{n} x_i c_i,\; c_2, \ldots, c_n\right) \\ &=\; \sum_{i=1}^{n} x_i \det\left(c_i, c_2, \ldots, c_n\right) \end{aligned}$$

But for any $i \neq 1$ in this sum the term $\det(c_i, c_2, \ldots, c_n)$ vanishes, as the column c_i appears in the determinant twice. Hence this sum boils down to the simple expression

$$0 \;=\; x_1 \det(c_1, c_2, \ldots, c_n) \;=\; x_1 \det(A)$$

Since $x_1 \neq 0$ by assumption and R is an integral domain this can only mean $\det(A) = 0$ such that we have proved (c) $\implies$ (a).

For the converse direction let us suppose that $\{\, c_1, c_2, \ldots, c_n \,\}$ is not linearly dependent, then we have to show that $\det(A) \neq 0$. To do this let us consider R to be a sub-ring of the quotient field $R \hookrightarrow E := \mathrm{QUOT}(R)$. Then $\{\, c_1, c_2, \ldots, c_n \,\}$ not only is R-linearly independent but even E-linearly independent: If we had

$$\frac{a_1}{b_1}c_1 + \frac{a_2}{b_2}c_2 + \ldots \frac{a_n}{b_n}c_n \;=\; 0$$

then we could multiply this equation by $b := b_1 b_2 \dots b_n \in R$ to find (note that $b \neq 0$, as all the $b_i \neq 0$ and $b/b_i \in R$ is a well-defined element of R) the following relation in R

$$a_1 \frac{b}{b_1} c_1 + a_2 \frac{b}{b_2} c_2 + \dots a_n \frac{b}{b_n} c_n \;=\; 0$$

As the c_i are R-linearly independent this would imply $a_i\, b/b_i = 0$ and hence $a_i = 0$ such that in turn $a_i/b_i = 0$ for any $i \in 1 \dots n$. Therefore $\{ c_1, c_2, \dots, c_n \}$ not only is E-linearly independent but, as E is a field, also an E-basis of E^n. Thus by (i).(e) we have $\det(A) \in E^* = E \setminus \{0\}$. In particular $\det(A) \neq 0$.

Since $\det(A^*) = \det(A)$ and the columns of A^* are just the rows of A we also find that (d) is equivalent to $\det(A^*) = 0$ which is again equivalent to (a). Thus we also have (d) $\iff$ (a).

□

Proof of (4.66):
If we abbreviate $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n) \in M^n$ and generalize the matrix-vector multiplication to M by writing

$$Ax \;:=\; \begin{pmatrix} \sum_{j=1}^n a_{1,j}\, x_j \\ \vdots \\ \sum_{j=1}^n a_{n,j}\, x_j \end{pmatrix}$$

then by assumption we have $Ax = y$. Since M is an R-module all the operations of R and M are compatible. E.g. if a, $b \in R$ and $x \in M$ then we have $a(bx) = (ab)x$. Consequentially we find

$$A^\# y \;=\; A^\#(Ax) \;=\; (A^\# A)x \;=\; \det(A)x$$

according to (4.63.(iii)). By definition the (i,j)-th entry $a^\#_{i,j}$ of the adjugate matrix $A^\#$ is the (j,i)-th coefficient of the cofactor matrix $C = (c_{i,j})$ of A, which is $c_{i,j} = (-1)^{i+j} \det(A_{i,j})$. Therefore

$$\det(A)x \;=\; A^\# y \;=\; \begin{pmatrix} \sum_{i=1}^n a^\#_{1,i}\, y_i \\ \vdots \\ \sum_{i=1}^n a^\#_{n,i}\, y_i \end{pmatrix} \;=\; \begin{pmatrix} \sum_{i=1}^n c_{i,1}\, y_i \\ \vdots \\ \sum_{i=1}^n c_{i,n}\, x_i \end{pmatrix}$$

But these are precisely the n equations given in the claim. Finally, as thereby $\det(A)x_j \in \mathrm{Lh}\{ y_1, \dots, y_n \}$ for any $j \in 1 \dots n$ it is clear that the entire sub-module generated by the $\det(A)x_j$ is contained in

$$\det(A) \cdot \mathrm{Lh}\{ x_1, x_2, \dots, x_n \} \quad\subseteq\quad \mathrm{Lh}\{ y_1, y_2, \dots, y_n \}$$

□

Proof of (2.4):

(i) Let us abbreviate $\mathfrak{u} := \bigcup \mathcal{A}$, as $\mathcal{A}$ is non-empty there is some $\mathfrak{a} \in \mathcal{A}$. And as $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ is an ideal we have $0 \in \mathfrak{a} \in \mathcal{A}$ and hence $0 \in \mathfrak{u}$. If now a, $b \in \mathfrak{u}$ then - by construction - there are $\mathfrak{a}$, $\mathfrak{b} \in \mathcal{A}$ such that $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$. As $\mathcal{A}$ is a chain we may assume $\mathfrak{a} \subseteq \mathfrak{b}$ and hence $a \in \mathfrak{b}$, too. Therefore we get $a + b \in \mathfrak{b}$ and $-a$, $-b \in \mathfrak{b}$, such that $a + b$, $-a$ and $-b \in \mathfrak{u}$ again. And if finally $r \in R$ then $ra \in \mathfrak{a}$, such that $ra \in \mathfrak{u}$.

(ii) Let $\mathcal{Z} := \{ \mathfrak{b} \trianglelefteq_{\mathfrak{i}} R \mid \mathfrak{a} \subseteq \mathfrak{b} \neq R \}$, then $\mathcal{Z} \neq \emptyset$ since $\mathfrak{a} \in \mathcal{Z}$. Now let $\mathcal{A} \subseteq \mathcal{Z}$ be a chain in $\mathcal{Z}$, then by (i) we know that $\mathfrak{u} := \bigcup \mathcal{A} \trianglelefteq_{\mathfrak{i}} R$ is an ideal of R. Suppose $\mathfrak{u} = R$, then $1 \in \mathfrak{u}$ and hence there would be some $\mathfrak{b} \in \mathcal{A}$ with $1 \in \mathfrak{b}$. But as $\mathfrak{b} \trianglelefteq_{\mathfrak{i}} R$ is an ideal this would mean $\mathfrak{b} = R$ in contradiction to $\mathfrak{b} \in \mathcal{A} \subseteq \mathcal{Z}$. Hence we find $\mathfrak{u} \in \mathcal{Z}$ again. But by construction we have $\mathfrak{b} \subseteq \mathfrak{u}$ for any $\mathfrak{b} \in \mathcal{A}$, that is $\mathfrak{u}$ is an upper bound of $\mathcal{A}$. Hence by the lemma of Zorn there is some maximal element $\mathfrak{m} \in \mathcal{Z}^*$. It only remains to show that $\mathfrak{m}$ is maximal: as $\mathfrak{m} \in \mathcal{Z}$ it is an non-full ideal $\mathfrak{m} \neq R$. And if $R \neq \mathfrak{b} \trianglelefteq_{\mathfrak{i}} R$ is another non-full ideal with $\mathfrak{m} \subseteq \mathfrak{b}$ then $\mathfrak{a} \subseteq \mathfrak{m} \subseteq \mathfrak{b}$ implies $\mathfrak{b} \in \mathcal{Z}$. But now it follows that $\mathfrak{b} = \mathfrak{m}$ since $\mathfrak{m} \in \mathcal{Z}^*$, $\mathfrak{b} \in \mathcal{Z}$ and $\mathfrak{m} \subseteq \mathfrak{b}$.

(iii) Let $a \in R^*$ be a unit of R and $\mathfrak{m} \trianglelefteq_{\mathfrak{i}} R$ be a maximal ideal. Then $a \notin \mathfrak{m}$, as else $1 = a^{-1}a \in \mathfrak{m}$ and hence $\mathfrak{m} = R$. From this we get $R^* \subseteq R \setminus \bigcup \mathrm{Smax}(R)$. For the converse inclusion we go to complements and prove $R \setminus R^* \subseteq \bigcup \mathrm{Smax}(R)$ instead. Thus let $a \in R$ be a non-unit $a \notin R^*$, then $1 \notin aR$ and hence $aR \neq R$. Thus by (i) there is a maximal ideal $\mathfrak{m} \trianglelefteq_{\mathfrak{i}} R$ containing $a \in aR \subseteq \mathfrak{m} \subseteq \bigcup \mathrm{Smax}(R)$. Thus we also have $a \in \bigcup \mathrm{Smax}R$ which had to be proved.

(iv) If $R = 0$ is the zero-ring, then $R = \{0\}$ is the one and only ideal of R. But as this ideal is full, it cannot be maximal and hence $\mathrm{Smax}(R) = \emptyset$. If $R \neq 0$ then $\mathfrak{a} := \{0\}$ is a non-full ideal of R. Hence by (ii) there is a maximal ideal $\mathfrak{m} \in \mathrm{Smax}(R)$ containing it. In particular $\mathrm{Smax}(R) \neq \emptyset$.

(v) If R is a field and $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$ is any ideal, then we distinguish two cases: If $\mathfrak{a} = 0$, then everything's fine. If $\mathfrak{a} \neq 0$ then there is some $a \in \mathfrak{a}$ with $a \neq 0$. Thus we have $1 = a^{-1}a \in \mathfrak{a}$ and thereby $\mathfrak{a} = R$. So the only ideal strictly larger than 0 is R itself and this makes 0 maximal. Note that $0 \neq R$, as in a field we have $0 \neq 1$.

If conversely 0 is a maximal ideal of R, then for any $a \in R$ with $a \neq 0$ we have $0 \subset aR \subseteq R$. That is aR is an ideal strictly larger, than 0. By maximality of 0 this means $aR = R$ and thereby there is some $b \in R$ such that $ab = 1$. This means a is a unit of R and as this is true for any $a \neq 0$, we found that R is a field.

□

Proof of (3.18):
Of course we will prove the claim using a Zornification: Let us define the collection of all proper sub-modules of N, that is

$$\mathcal{Z} \;:=\; \{ Z \leq_{\mathfrak{m}} N \mid P \subseteq Z, Z \neq N \}$$

As $P \in \mathcal{Z}$ this collection is non-empty. Also it is clear that $\mathcal{Z}$ is partially ordered under the inclusion relation "$\subseteq$". If now $(Z_i) \subseteq \mathcal{Z}$ is a chain in $\mathcal{Z}$ (that is a totally ordered subset), we take $Z := \bigcup_i Z_i$. Then $Z \leq_{\mathfrak{m}} N$ is a sub-module again: if $x, y \in Z$ then there are some $i, j \in I$ such that $x \in Z_i$ and $y \in Z_j$. As these sets are totally ordered we may assume $Z_i \subseteq Z_j$ without loss of generality. And hence $x + y \in Z_j \subseteq Z$ again. Also if $a \in R$, then $ax \in Z_i \subseteq Z$.

Now suppose $Z = N$, in particular for any $k \in 1 \ldots n$ we have $x_j \in N = Z$. Therefore for any $k \in 1 \ldots n$ there is some $i(k) \in I$ such that $x_k \in Z_{i(k)}$. As the Z_i are totally ordered we may single out the maximal element among $Z_{i(1)}, \ldots, Z_{i(n)}$. That is there is some $j \in I$ such that $Z_{i(k)} \subseteq Z_j$ for any $k \in 1 \ldots n$. In particular $x_k \in Z_{i(k)} \subseteq Z_j$ and as Z_j is an R-module we find $\mathrm{Lh}\{ x_1, \ldots, x_n \} \subseteq Z_j$. Now, as also $P \subseteq Z_j$ we get $N = P + \mathrm{Lh}\{ x_1, \ldots, x_n \} \subseteq Z_j \subseteq N$, that is $Z_j = N$. But this is in contradiction to

$Z_j \in \mathcal{Z}$, such that we necessarily have $Z \neq N$.

Let us subsume: we have found a sub-module $Z \leq_{\mathsf{m}} N$ with $Z \neq N$ and clearly also $P \subseteq Z$. That is $Z \in \mathcal{Z}$ again. But by construction Z is an upper bound (for any $i \in I$ we have $Z_i \subseteq Z$) of the chain (Z_i). Hence we may apply Zorn's lemma to find a maximal element $M \in \mathcal{Z}^*$. So by construction of $M \in \mathcal{Z}$ we have properties (1) and (2) of the claim. And if $M \subseteq Q \subseteq N$ for some sub-module Q, then either $Q = N$ or $Q \in \mathcal{Z}$ and hence $M = Q$, due to the maximality of M, and this is (3). □

Proof of (3.57):

(i) Because of (D1) (that is $x \in T \implies T \vdash x$) we have the obvious inclusions $S \subseteq T \subseteq \langle T \rangle$. That is we have $T \vdash S$. If now $x \in M$ with $S \vdash x$, then by (D2) we also get $T \vdash x$. And this is just a reformulation of the claim $\langle S \rangle \subseteq \langle T \rangle$.

(ii) We will first prove $\langle S \rangle = \bigcap \{ P \in \mathrm{sub}(M) \mid S \subseteq P \}$. For the inclusion "$\subseteq$" we are given any $x \in \langle S \rangle$. Then we need to show that for any $P \in \mathrm{sub}(M)$ with $S \subseteq P$ we get $x \in P$. As $P \in \mathrm{sub}(M)$ there is some $T \subseteq M$ with $P = \langle T \rangle$. Then $S \subseteq P$ translates into $S \subseteq \langle T \rangle$, which is $T \vdash S$. Together with $S \vdash x$ now property (D2) implies $T \vdash x$. And this is $x \in \langle T \rangle = P$, which had to be shown. Conversely for "$\supseteq$" we are given some $x \in M$ such that for any $P \in \mathrm{sub}(M)$ we get $S \subseteq P \implies x \in P$. Then we may simply choose $P := \langle S \rangle$, then $S \subseteq P$ is satisfied due to (D1). Thus by assumption on x we get $x \in P = \langle S \rangle$, which had to be shown.

Thus let us now prove $P = \langle P \rangle$, where we abbreviated $P := \langle S \rangle$. The inclusion "$\subseteq$" is clear by (D1) again. And by what we have shown, we have $\langle P \rangle = \bigcap \{ Q \in \mathrm{sub}(M) \mid P \subseteq Q \}$. But as $P \in \mathrm{sub}(M)$ with $P \subseteq P$ this trivially yields $\langle P \rangle \subseteq P$, the converse inclusion.

(iii) (a) $\implies$ (c): by assumption there is some $s \in S$ such that $S \setminus \{ s \} \vdash s$. Due to (D3) there is some finite subset $S_s \subseteq S \setminus \{ s \}$ such that $S_s \vdash s$. Now let $S_0 := S_s \cup \{ s \}$, then S_0 is finite again, as $\#S_0 = \#S_s + 1 < \infty$ and $S_0 \setminus \{ s \} = S_s$. In particular $S_0 \setminus \{ s \} \vdash s$, that is S_0 is $\vdash$depenedent. (c) $\implies$ (b): consider $S_0 \subseteq S \subseteq T$, by assumption there is some $s \in S_0$ such that $S_0 \setminus \{ s \} \vdash s$. However $S_0 \setminus \{ s \} \subseteq T \setminus \{ s \}$, such that by (i) we also get $T \setminus \{ s \} \vdash s$. That is T is $\vdash$dependent. (b) $\implies$ (a) finally is trivial, by letting $T := S$.

(iv) (a) $\implies$ (b): suppose S was $\vdash$dependent, that is there was some $s \in S$, such that $S \setminus \{ s \} \vdash s$. As $S \subseteq T$ we also have $S \setminus \{ s \} \subseteq T \setminus \{ s \}$, hence we find $S \setminus \{ s \} \vdash s$ due to (i). But as also $s \in S \subseteq T$ this is a contradiction to T being $\vdash$independent. (b) $\implies$ (c) is trivial (a finite subset is a subset). (c) $\implies$ (a): suppose there was some $x \in T$ such that $T \setminus \{ x \} \vdash x$. Then by (D3) there would be a finite subset $T_x \subseteq T \setminus \{ x \}$ such that $T_x \vdash x$. Now let $T_0 := T_x \cup \{ x \}$, then T_0 is finite again, as $\#T_0 = \#T_x + 1 < \infty$. Also $T_0 \setminus \{ x \} = T_x \vdash x$, that is T_0 is $\vdash$dependent in contradiction to (c).

(v) (b) $\implies$ (a): clearly $S \subset T := S \cup \{ x \}$, such that S is $\vdash$independent by assumption (a) and (iv). Now suppose we had $S \vdash x$, then clearly $T \setminus \{ x \} = S \vdash x$. That is T is $\vdash$dependent in contradiction to the assumption. (a) $\implies$ (b): if we had $x \in S$, then by property (D1) also $S \vdash x$, in contradiction to the assumption. Now suppose that $S \cup \{ x \}$ was $\vdash$dependent. That is there

would be some $s \in S \cup \{ x \}$ such that

$$S' \;:=\; \Big(S \cup \{ x \}\Big) \setminus \{ s \} \;\vdash\; s$$

We now distinguish two cases: (1) if $s = x$ then $S' = S$ and thereby we would get $S = S' \vdash s = x$, a contradiction to $S \nvdash x$. (2) if $s \neq x$ then $s \in S \cup \{ x \}$ implies $s \in S$. Now let $R := S \setminus \{ s \}$, that is $S = R \cup \{ s \}$ and $S' = (S \cup \{ x \}) \setminus \{ s \} = R \cup \{ x \}$. This again means

$$S' \setminus \{ x \} \;=\; R \;=\; S \setminus \{ s \}$$

As S is $\vdash$independent we now have $S' \setminus \{ x \} = S \setminus \{ s \} \nvdash s$. Because of $x \in S'$, $S' \vdash s$ and $S' \setminus \{ x \} \nvdash s$ property (D4) implies

$$S \;=\; \Big(S \setminus \{ s \}\Big) \cup \{ s \} \;=\; \Big(S' \setminus \{ x \}\Big) \cup \{ s \} \;\vdash\; x$$

This is a contradiction to $S \nvdash x$ again, thus in both cases we have derived a contradiction, that is $S \cup \{ x \}$ is $\vdash$independent, as claimed.

(vi) Let us abbreviate the chain's union by $T := \bigcup_i S_i$ and suppose T would be $\vdash$dependent. Then by (iii) there would be a finite subset $T_0 \subseteq T$, such that T_0 is $\vdash$dependent, already. Say $T_0 = \{ x_1, \ldots, n_n \}$, where for any $k \in 1 \ldots n$ we have $x_k \in S_{i(k)}$ for some $i(k) \in I$. As $\{ S_i \mid i \in I \}$ is totally ordered under $\subseteq$, so is the finite subset $\Big\{ S_{i(k)} \mid k \in 1 \ldots n \Big\}$. Without loss of generality we may assume, that $S_{i(n)}$ is the maximal element among the $S_{i(k)}$. Hence we find $x_k \in S_{i(k)} \subseteq S_{i(n)}$ for any $k \in 1 \ldots n$ and this again means $T_0 \subseteq S_{i(n)}$. Yet as T_0 was $\vdash$dependent this implies, that $S_{i(n)}$ is $\vdash$dependent (by (iii) again), a contradiction. Hence T is $\vdash$independent, as claimed.

(vii) Not surprisingly we will prove the claim using a zornification based on

$$\mathcal{Z} \;:=\; \{ P \subseteq M \mid S \subseteq P \subseteq T,\ P \text{ is } \vdash\text{independent} \}$$

Of course $\mathcal{Z}$ is non-empty, as $S \in \mathcal{Z}$, and it is partially ordered under the inclusion relation $\subseteq$. Due to (vi) any ascending chain (S_i) admits an upper bound, namely $T := \bigcup_i S_i \in \mathcal{Z}$. Thus by the lemma of Zorn $\mathcal{Z}$ contains a maximal element B. Because of $B \in \mathcal{Z}$ we have $S \subseteq B \subseteq T$ and B is $\vdash$independent. Now suppose there was some $x \in T$ with $B \nvdash x$. However, as B is $\vdash$independent and $B \nvdash x$, we find by (v) that even $B \cup \{ x \}$ is $\vdash$independent. But as $x \notin B$ we have $B \subset B \cup \{ x \} \subseteq T$. Thus we have found a contradiction to the maximality of B. This contradiction can only be solved, if $T \subseteq \langle B \rangle$. And using (i) and (ii) we thereby get $M = \langle T \rangle \subseteq \langle \langle B \rangle \rangle = \langle B \rangle \subseteq M$. Altogether B is $\vdash$ independent and $M = \langle B \rangle$ - it is a $\vdash$basis.

(viii) First suppose $x = b$, then $B' = B$ and hence there is nothing to show. Thus assume $x \neq b$. The proof now consists of two parts: (1) as $B \setminus \{ b \} \subseteq B' \subseteq \langle B' \rangle$ and $B' \vdash b$ by assumption, we have $B = (B \setminus \{ b \}) \cup \{ b \} \subseteq \langle B' \rangle$. And thereby $M = \langle B \rangle \subseteq \langle \langle B' \rangle \rangle = \langle B' \rangle \subseteq M$, according to (ii). That is $M = \langle B' \rangle$. (2) as $B \setminus \{ b \} \subseteq B$ is a subset and B is $\vdash$independent, so is $B \setminus \{ b \}$, due to (iv). Now suppose $B \setminus \{ b \} \vdash x$, then we would get $B' = (B \setminus \{ b \}) \cup \{ x \} \subseteq \langle B \setminus \{ b \} \rangle$. And hence $b \in M = \langle B' \rangle \subseteq \langle \langle B \setminus \{ b \} \rangle \rangle = \langle B \setminus \{ b \} \rangle$, according to (1) and (ii) once more. But this is $B \setminus \{ b \} \vdash b$ in contradiction to the $\vdash$independence of B. Thus we have $B \setminus \{ b \} \nvdash x$, as $B \setminus \{ b \}$

also is $\vdash$independent (v) now implies, that $B' = (B \setminus \{ b \}) \cup \{ x \}$ is $\vdash$independent. Combining (1) and (2) we found that B' is a $\vdash$basis.

(ix) (a) $\implies$ (b): $M = \langle B \rangle$ is clear by definition of a $\vdash$basis. Now consider some subset $S \subset B$, that is there is some $x \in B$, with $x \notin S$. As B is $\vdash$independent and $x \in B$ we get $B \setminus \{ x \} \nvdash x$, in other words $x \notin \langle B \setminus \{ x \} \rangle$. And as $S \subseteq B \setminus \{ x \}$ (i) implies $x \notin \langle S \rangle$. In particular $\langle S \rangle \neq M$, as claimed.

(b) $\implies$ (a): as $M = \langle B \rangle$ by assumption it only remains to verify the $\vdash$independence of B. Thus assume, there was some $x \in B$ such that $S := B \setminus \{ x \} \vdash x$. As $S \subseteq \langle S \rangle$ and $x \in \langle S \rangle$, we have $B = S \cup \{ x \} \subseteq \langle S \rangle$. And thereby $M = \langle B \rangle \subseteq \langle \langle S \rangle \rangle = \langle S \rangle \subseteq M$ according to (ii). This is $M = \langle S \rangle$ even though $S \subset B$, a contradiction.

(ix) (a) $\implies$ (c): suppose B is a $\vdash$basis, that by definition B already is $\vdash$independent. Thus suppose $B \subset S$, that is we may choose some $s \in S \setminus B$. As $s \in M = \langle B \rangle$ we get $B \vdash s$. And as $B \subseteq S \setminus \{ s \}$ (i) also yields $S \setminus \{ s \} \vdash s$. That is S is $\vdash$ dependent, as claimed.

(c) $\implies$ (a): as B is assumed to be $\vdash$independent, it remains to show $M = \langle B \rangle$. Thus suppose we had $\langle B \rangle \subset M$, that is there was some $s \in M$ such that $B \nvdash s$. Then by (v) we find that $S := B \cup \{ s \}$ is independent, as well - a contradiction.

(x) Let us abbreviate $B' := (B \setminus A) \cup A'$, then we first prove, that B' also generates M. So consider any $x \in M$, as B is a basis we have $B \vdash x$ and by (D2) there are finitely many elements $a_1, \ldots, a_m \in A$ and $b_1, \ldots, b_n \in B \setminus A$ such that

$$\{ a_1, \ldots, a_m, b_1, \ldots, b_n \} \vdash x$$

For any $i \in 1 \ldots m$ we have $a_i \in A \subseteq \langle A \rangle = \langle A' \rangle$ such that $A' \vdash a_i$. And as this is true for any i we have $A' \vdash \{ a_i, \ldots, a_m \}$. According to (i) in particular $A' \cup \{ b_1, \ldots, b_n \} \vdash \{ a_i, \ldots, a_m \}$. But as $b_i \in A' \cup \{ b_1, \ldots, b_n \}$ we also get $A' \cup \{ b_1, \ldots, b_n \} \vdash \{ b_1, \ldots, b_n \}$ by (D1). Altogether

$$A' \cup \{ b_1, \ldots, b_n \} \vdash \{ a_1, \ldots, a_m, b_1, \ldots, b_n \}$$

We now use property (D3) to find $A' \cup \{ b_1, \ldots, b_n \} \vdash x$. By (i) again, that is $B' = A' \cup (B \setminus A) \vdash x$ and as this is true for any $x \in M$ we have $B' \vdash M$ which makes B' a generating set of M.

It remains to prove, that B' also is $\vdash$independent. Suppose not, then by (iii) there would be a finite subset of B' that is $\vdash$dependent. In this case there are some $a'_1, \ldots, a'_m \in A'$ and $b_1, \ldots, b_n \in B \setminus A$ such that $\{ a'_1, \ldots, a'_m, b_1, \ldots, b_n \}$ was $\vdash$dependent. We choose $n \in \mathbb{N}$ minimal such that

$$\exists\, b_1, \ldots, b_n \in B \setminus A \ : \ A' \cup \{ b_1, \ldots, b_n \} \quad \text{is } \vdash\text{dependent}$$

Clearly $n = 0$ is absurd, as this would mean that A' is $\vdash$dependent, which we assumed not to be the case. So $n \geq 1$, but as n is minimal, this means $A' \cup \{ b_2, \ldots, b_n \}$ is $\vdash$independent. Now from $A' \cup \{ b_1, \ldots, b_n \}$ being $\vdash$dependent (v) yields

$$A' \cup \{ b_2, \ldots, b_n \} \vdash b_1$$

Again for any $a' \in A'$ we have $a' \in A' \subseteq \langle A' \rangle = \langle A \rangle$ such that $A \vdash a'$. And as this is true for any $a' \in A'$ even $A \vdash A'$. In particular $A \cup \{ b_2, \ldots, b_n \} \vdash A'$ by (i) again. As before by (D1) $b_j \in A \cup \{ b_2, \ldots, b_n \}$ implies $A \cup \{ b_2, \ldots, b_n \} \vdash b_j$ for any $j \in 2 \ldots n$. Together we have

$$A \cup \{ b_2, \ldots, b_n \} \ \vdash \ A' \cup \{ b_2, \ldots, b_n \}$$

so we find $A \cup \{ b_2, \ldots, b_n \} \vdash b_1$ according to (D3). In particular $A \cup \{ b_1, b_2, \ldots, b_n \}$ is $\vdash$dependent in contradiction to the larger set B being $\vdash$independent. This contradiction can only be solved by B' being $\vdash$independent and hence B is a basis of M.

(xi) Let us denote $m := |A|$ and $n := |B|$, then we need to show $m = n$. In the proof we will have to distinguish two cases: (I) m or n is finite and (II) both m and n are infinite. We will deal with (I) in the following steps (1) to (4), whereas (II) will be treated in (5)

(1) Without loss of generality we may assume $m \leq n$ (interchanging A and B if not). Then M is finite by assumption (I), let us denote the elements of A by $A = \{ x_1, \ldots, x_m \}$. Thereby let us assume that $x_1, \ldots, x_k \notin B$ and $x_{k+1}, \ldots, x_m \in B$ for some $k \in \mathbb{N}$ [note that for $k = 0$ this is $A \subseteq B$ and for $k = m$ this is $A \cap B = \emptyset$]. In the case $k = 0$ we may skip steps (2), (3) and let $A^{(k)} := A$, immediately proceeding with (4).

(2) As A is a $\vdash$basis of M, it is a minimal $\vdash$generating subset, by (ix). That is $\langle \{ x_2, \ldots, x_m \} \rangle \neq M = \langle B \rangle$. Hence there is some point $b \in B$ such that $b \notin \langle \{ x_2, \ldots, x_m \} \rangle$ [as else $B \subseteq \langle \{ x_2, \ldots, x_m \} \rangle$ and hence $M = \langle B \rangle \subseteq \langle \langle \{ x_2, \ldots, x_m \} \rangle \rangle = \langle \{ x_2, \ldots, x_m \} \rangle$, according to (ii), a contradiction]. For this $b \in B$ let us define

$$A' \ := \ \Big(A \cup \{ b \} \Big) \setminus \{ x_1 \} \ = \ \{ b, x_2, \ldots, x_m \}$$

Then A' is $\vdash$independent [as A is $\vdash$independent, the same is true for $\{ x_2, \ldots, x_m \}$. And due to $\{ x_2, \ldots, x_m \} \nvdash b$ (v) implies, that A' is independent]. Next we find that $A' \vdash x_1$ [because if we had $A' \nvdash x_1$ then - using (v) and the fact that A' is $\vdash$independent - $A' \cup \{ x_1 \}$ would be $\vdash$independent, too. However this is untrue, as $(A' \cup \{ x_1 \}) \setminus \{ b \} = A \vdash b$]. Therefore A' even is a $\vdash$basis [as $A' \vdash x_1$ we have $x_1 \in \langle A' \rangle$ and clearly $A \setminus \{ x_1 \} \subseteq \langle A' \rangle$, such that $A = (A \setminus \{ x_1 \}) \cup \{ x_1 \} \subseteq \langle A' \rangle$. Combined with (ii) this yields $M = \langle A \rangle \subseteq \langle \langle A' \rangle \rangle = \langle A' \rangle \subseteq M$, that is $\langle A \rangle = M$ and the $\vdash$independence of A' has already been shown].

(3) In (2) we have replaced $x_1 \in A$ by some $b \in B$ to obtain another $\vdash$basis $A' := (A \cup \{ b \}) \setminus \{ x_1 \} = \{ b, x_2, \ldots, x_k \}$. That is: venturing from A to A' we have increased the number of elements in $A' \cap B$ by 1 (with respect to $A \cap B$). Iterating this process k times we establish a $\vdash$basis $A^{(k)} = \{ b_1, \ldots, b_k, x_{k+1}, \ldots, x_m \} \subseteq B$.

(4) From the construction it is clear, that $|A'| \leq m \leq n = |B|$. On the other hand - as B is a $\vdash$basis, $A' \subseteq B$ and $M = \langle A' \rangle$ - item (ix) now implies that $A' = B$. And thereby $n = |B| = |A'| \leq m$, as well. Together this is $m = n$ as claimed.

(5) It remains to regard case (II), that is m and N are both infinite. As $B \subseteq M = \langle A \rangle$ we obviously have $A \vdash b$ for any $b \in B$. Thus by property (D3) there is a subset $A_b \subseteq A$ such

that $\#A_b < \infty$ is finite and $A_b \vdash b$ already. Now let

$$A^* \;:=\; \bigcup_{b\in B} A_b \quad\subseteq\quad A$$

Then for any $b \in B$ we have $A_b \subseteq A^*$ and hence $A^* \vdash b$, due to (i). That is $b \in \langle A^* \rangle$ for any $b \in B$ and hence $B \subseteq \langle A^* \rangle$. Thus by (i) and (ii) again we get $M = \langle B \rangle \subseteq \langle \langle A^* \rangle \rangle = \langle A^* \rangle \subseteq M$, such that $M = \langle A^* \rangle$. Now, as A is a $\vdash$basis, if we had $A^* \subset A$, then (ix) would yield $M \neq \langle A^* \rangle$, a contradiction. This is $A = A^*$ and hence we may compute

$$|A| \;=\; \left| \bigcup_{b\in B} A_b \right| \;\leq\; \sum_{b\in B} |A_b| \;\leq\; |B \times \mathbb{N}| \;=\; |B|$$

Hereby $|B \times \mathbb{N}| = |B|$ holds true, as B was assumed to be infinite. Thus we have found $m \leq n$ and by interchanging the roles of A and B we also find $n \leq m$, which had to be shown.

(xii) As S is independent, $S \subseteq M$ and $M = \langle M \rangle$ we get from (vii) that there is some $\vdash$basis A of M, with $S \subseteq A \subseteq M$. Thus by (x) we already obtain the claim from $|S| \leq |A| = |B|$. Likewise, as T generates M and $\emptyset$ is independent (trivially), we get from (vii) that there is some $\vdash$basis A of M, with $\emptyset \subseteq A \subseteq T$. Thus by (x) we already obtain the claim from $|B| = |A| \leq |T|$.

(xiii) (b) $\implies$ (a) has already been shown in (x), thus it only remains to verify (a) $\implies$ (b): thus consider any $\vdash$independent subset $S \subseteq M$ with $|S| = |B|$. As before [S is independent, $S \subseteq M$ and $M = \langle M \rangle$ now use (vii)] there is some $\vdash$basis A of M, with $S \subseteq A \subseteq M$. Thus by (x) we find $|B| = |S| \leq |A| = |B|$. That is $|A| = |S| = |B| < \infty$ which was assumed to be finite. In particular S is a subset of the finite set A, with the same number of elements $\#S = \#A$. Clearly this means $S = A$ and in particular S is a $\vdash$basis of M.

□

Proof of (3.60):

(i) Trivially $\emptyset$ is R-linearly independent and $\emptyset$ also generates $\{0\}$, as $\{0\}$ is the one and only submodule of $\{0\}$. Together $\emptyset$ is an R-basis of $\{0\}$ and in particular $\mathrm{rank}\{0\} = 0$. Conversely if $\mathrm{rank} M = 0$, then by definition $M = \langle \emptyset \rangle_{\mathsf{m}} = \{0\}$.

(ii) If $M = P + \langle X \rangle_{\mathsf{m}}$ then as $P \subseteq Q$ we also get $M = Q + \langle X \rangle_{\mathsf{m}}$.

(iii) First suppose $\mathfrak{a} = aR$ is principal. If $a = 0$, then $\mathfrak{a} = 0$, which is a free R-module, with basis $\emptyset$. And if $a \neq 0$, then $\{\, a \,\}$ is an R-basis of $\mathfrak{a}$. It generates $\mathfrak{a}$, as $\langle \{\, a \,\} \rangle_{\mathsf{m}} = aR = \mathfrak{a}$ and it is R-linearly independent, as $ba = 0 \implies b = 0$ (as $a \neq 0$ and R is an integral domain). Conversely suppose $\mathfrak{a}$ is free, with basis $B \subseteq \mathfrak{a}$. If $B = \emptyset$, then $\mathfrak{a} = \langle \emptyset \rangle_{\mathsf{m}} = 0$, which is principal $\mathfrak{a} = 0 = R0$. And if we had $\#B \geq 2$, then we could choose some $b_1, b_2 \in B$. But this would yield $b_2 b_1 + (-b_1) b_2 = 0$ (as R is commutative) and hence B would not be R-linearly independent. Thus it only remains $\#B = 1$, say $B = \{\, a \,\}$ and hence $\mathfrak{a} = \langle B \rangle_{\mathsf{m}} = aR$ is principal.

(iv) We have to prove that E is an R-linearly independent set, that also R-generates $R^{\oplus I}$. Thus suppose we are given any $x = (x_i) \in R^{\oplus I}$. Let us denote $\Omega := \{\, i \in I \mid x_i \neq 0 \,\}$, then Ω is finite,

by definition of $R^{\oplus I}$. And hence we get $x = \sum_{i\in\Omega} x_i e_i \in \langle \mathcal{E} \rangle_{\mathfrak{m}}$. Therefore $\mathcal{E}$ generates $R^{\oplus I}$ as an R-module. For the R-linear independence we have $\sum_{i\in\Omega} a_i e_i = 0$ for some finite subset $\Omega \subseteq I$ and some $a_i \in R$. We now compare the coefficients of 0 and $\sum_{i\in\Omega} a_i e_i$. Hereby for any $i \in \Omega$ the i-th coefficient of $0 \in R^{\oplus I}$ is $0 \in R$. And the i-th coefficient of $\sum_{i\in\Omega} a_i e_i$ is a_i. That is $a_i = 0$ for any $i \in \Omega$ and this means that $\mathcal{E}$ is R-linearly independent.

□

Proof of (3.61):

(i) (D1): consider an arbitrary subset $X \subseteq M$ and $x \in X$. Then we find $X \vdash x$ simply by choosing $n := 1$, $x_1 := x$ and $a_1 := 1$, as in this case $a_1 x_1 = 1x = x$. (D2): consider any two subsets X, $Y \subseteq M$ such that $Y \vdash X$ and $X \vdash x$. Thus by definition there are some $n \in \mathbb{N}$, $x_i \in X$ and $a_i \in R$ such that $x = a_1 x_1 + \cdots + a_n x_n$. But as $x_i \in X$ and $Y \vdash X$ there also are some $m(i) \in \mathbb{N}$, $y_{i,j} \in Y$ and $b_{i,j} \in R$ such that $x_i = b_{i,1} y_{i,1} + \cdots + b_{i,m(i)} y_{i,m(i)}$. Combining these equations, we find

$$x \;=\; \sum_{i=1}^{n} a_i x_i \;=\; \sum_{i=1}^{n} \sum_{j=1}^{m(j)} a_i b_{i,j} y_{i,j}$$

In particular this identity yields $Y \vdash x$, which had to be shown. (D3): consider an arbitrary subset $X \subseteq M$ and $x \in M$ such that $X \vdash x$. Again this means $x = a_1 x_1 + \cdots + a_n x_n$ for sufficient $x_i \in X$ and $a_i \in R$. Now let $X_0 := \{ x_1, \ldots, x_n \} \subseteq X$. Then X_0 clearly is a finite set and $X_0 \vdash x$, by construction. As (D1), (D2) and (D3) are satisfied, we already obtain (iii), (iv) and (v) from (3.57).

(ii) The identity $\langle X \rangle = \{ x \in M \mid X \vdash x \} = \mathrm{Lh}_R(X)$ is obvious from the definitions of the relation $\vdash$ and the linear hull $\mathrm{Lh}_R(X)$. And the identity $\mathrm{Lh}_R(X) = \langle X \rangle_{\mathfrak{m}}$ has already been shown in (3.12).

(vi) (b) $\Longrightarrow$ (a): we first prove that B is a *generating system* of M: Thus consider any $x \in M$, by assumption there is some $(x_b) \in R^{\oplus B}$ such that $x = \sum_b x_b b$. Now let $\Omega := \{ b \in B \mid x_b \neq 0 \}$. Then $\Omega \subseteq B$ is finite and we further get

$$x \;=\; \sum_{b\in B} x_b b \;=\; \sum_{b\in\Omega} x_b b \;\in\; \mathrm{Lh}_R(B)$$

As x has been arbitrary that is $M \subseteq \mathrm{Lh}_R(B) = \langle B \rangle_{\mathfrak{m}}$. Let us now prove that B also is *R-linear independent*: thus consider some finite subset $\Omega \subseteq B$ and some $a_b \in R$ (where $b \in \Omega$) such that $\sum_{b\in\Omega} a_b b = 0$. Then for any $b \in B \setminus \Omega$ we let $a_b := 0$ and thereby obtain

$$\sum_{b\in B} a_b b \;=\; \sum_{b\in\Omega} a_b b \;=\; 0 \;=\; \sum_{b\in B} 0 b$$

Due to the uniqueness of this representation (of $0 \in M$) we find $a_b = 0$ for any $b \in B$. And in particular $a_b = 0$ for any $b \in \Omega$. By definition this means that B truly is R-linearly independent.

(vi) (a) $\Longrightarrow$ (b): *Existence*: consider any $x \in M$, as $M = \langle B \rangle_{\mathfrak{m}} = \mathrm{Lh}_R(B)$ there are a finite subset $\Omega \subseteq B$ and $a_b \in R$ (where $b \in \Omega$) such that $x = \sum_{b\in\Omega} a_b b$. Now let $x_b := a_b$ if $b \in \Omega$ and $x_b := 0$ if $b \in B \setminus \Omega$. Then $(x_b) \in R^{\oplus B}$ and we also get

$$x \;=\; \sum_{b\in\Omega} a_b b \;=\; \sum_{b\in B} x_b b$$

Uniqueness: consider any two (x_b), $(y_b) \in R^{\oplus B}$ representing the same element $\sum_b x_b b = \sum_b y_b b$. Now let $\Omega := \{\, b \in B \mid x_b \neq 0, \text{ or } y_b \neq 0 \,\}$. Then $\Omega \subseteq B$ is finite and we clearly get

$$0 \;=\; \sum_{b\in B}(x_b - y_b)b \;=\; \sum_{b\in\Omega}(x_b - y_b)b$$

Yet as B is R-linearly independent, this means $x_b - y_b = 0$ for any $b \in \Omega$ and hence $x_b = y_b$ for any $b \in B$ (if $b \notin \Omega$, then $x_b = 0 = y_b$). But this already is the uniqueness of the representation.

□

Proof of (3.64):
As (3.66) is a direct continuation of (3.64) this proof deals with both of these propositions simultaneously. Hence the odd enumeration of the statements in (3.66) that began by (vii) instead of (i).

(i) By (3.61) $\vdash$ already satisfies (D1), (D2) and (D3). Thus it only remains to prove (D4) and we will already do this in the stronger form given in the claim. That is we consider $x \in X$ and $X \vdash y$. By definition of $\vdash$ this is $y = a_1x_1 + \cdots + a_nx_n$ for some $a_i \in S$ and $x_i \in X$. Of course we may drop any summand with $a_i = 0$ and hence assume $a_i \neq 0$ for any $i \in 1\ldots n$. As $y \neq 0$ we still have $n \geq 1$. Now let $X' := (X \setminus \{\, x \,\}) \cup \{\, y \,\}$ (that is we have to show $X' \vdash x$) and distinguish two cases: (1) if $x \notin \{\, x_1, \ldots, x_n \,\}$ then $\{\, x_1, \ldots, x_n \,\} \subseteq X \setminus \{\, x \,\} \subseteq X'$ and in particular $X' \vdash x$. (2) if $x \in \{\, x_1, \ldots, x_n \,\}$ we may assume $x = x_1$ without loss of generality. Now let $b_i := -a_1^{-1}a_i \in S$ (for any $i \in 2\ldots n$), then $x = x_1 = a_1^{-1}a_1x_1 = b_2x_2 + \cdots + b_nx_n$. And as $\{\, x_2, \ldots, x_n \,\} \subseteq X \setminus \{\, x \,\} \subseteq X'$ this implies $X' \vdash x$. Thus we have proved the claim in both cases. From this property we can easily derive (D4): suppose $x \in X$, $X \vdash y$ and $X \setminus \{\, x \,\} \nvdash y$. Then $y \neq 0$, as even $\emptyset \vdash 0$ and hence $X \setminus \{\, x \,\} \vdash y$. Thus we may apply this property to find $X' \vdash x$, which had to be shown.

(ii) (b) $\Longrightarrow$ (a): suppose there was some $x \in X$ such that $X \setminus \{\, x \,\} \vdash x$. So by definition there would be some elements $x_i \in X \setminus \{\, x \,\}$ and $a_i \in S$ (where $i \in 1\ldots n$) such that $x = a_1x_1 + \cdots + a_nx_n$. Now let $x_0 := x$ and $a_0 := -1$, then we get $x_i \in X$ for any $i \in 1\ldots n$ and also $a_0x_0 + a_1x_1 + \cdots + a_nx_n = 0$. But as $a_0 \neq 0$ this means that X is S-linear dependent, a contradiction. Thus there is no such $x \in X$ and this is the $\vdash$independence of X.

(a) $\Longrightarrow$ (b): suppose there were some (pairwise distinct) elements $x_i \in X$ and $a_i \in R$ (where $i \in 1\ldots n$) such that (without loss of generality) $a_1 \neq 0$ and $a_1x_1 + \cdots + a_nx_n = 0$. As $a_1 \neq 0$ we may let $b_i := -a_1^{-1}a_i$ for $i \in 2\ldots n$. Then $x_1 = a_1^{-1}a_1x_1 = b_2x_2 + \cdots + b_nx_n$ and hence $\{\, x_2, \ldots, x_n \,\} \vdash x_1$. As $\{\, x_2, \ldots, x_n \,\} \subseteq X \setminus \{\, x_1 \,\}$ this yields $X \setminus \{\, x_1 \,\} \vdash x_1$, that is X is $\vdash$dependent, a contradiction. Thus there are no such x_i and a_i and this again means, that X is S-linearly indepenendent.

(iv) As $\langle B \rangle = \mathrm{Lh}_S(B)$ S-generation and $\vdash$-generation are equivalent notions. And in (ii) we have seen that $\vdash$dependence and S-linear dependence are eqivalent, too. In particular we find (a) $\Longleftrightarrow$ (b) according to the respective definitions of S-bases and $\vdash$bases. And the equivalences (a) $\Longleftrightarrow$ (c) $\Longleftrightarrow$ (d) have already been proved in (3.57.(ix)). Finally the we have already shown (b) $\Longleftrightarrow$ (e) in (3.61.(vi)).

(iii) This is just a reformulation of (3.57.(v)) in the light of (ii). Likewise (v) resp. (vi) is just the content of (3.57.(vii)) resp. (3.57.(xi)) using the equivalences (a) $\Longleftrightarrow$ (b) of (iv). Finally (vii) and (viii) are

repetitions of (3.57.(xii)) and (3.57.(xiii)) respectively. All we did was bringing the definition of the dimension into play.

(ix) If $P \leq_{\mathfrak{m}} M$ then (according to (v)) we may pick up a basis B of P. Then by assumption $|B| = \dim(P) = \dim(V)$ and M is finitely generated. Now by (viii) we find that B even is an S-basis of M, as $|B| = \dim(M)$. In particular that is $P = \mathrm{Lh}(B) = M$.

□

Proof of (3.62):

(i) Say $B = \{ m_j \mid j \in J \}$ for some index set J and let $I \subseteq J$ be the index set, such that we then get $A = \{ m_i \mid i \in I \}$. Let us first prove, that $B/P := \{ m_j + P \mid j \in J \setminus I \}$ generates M/P. To do this consider any $x \in M$, then

$$x \;=\; \sum_{j \in J} x_j m_j$$

If we take this modulo $P = \mathrm{Lh}_R \{ m_i \mid i \in I \}$, then all the m_i for some $i \in I$ are eliminated, as $m_i + P = 0 + P$. Thus the sum breaks down to

$$x + P \;=\; \sum_{j \in J} x_j (m_j + P) \;=\; \sum_{j \in J \setminus I} x_j (m_j + P)$$

So we have found some coefficients $x_j \in R$ such that $x + P$ can be written as a linear combination over the $m_j + P$ where $j \in J \setminus I$. Now it remains to prove the linear independence: Consider any $b_j \in R$ (where $j \in J \setminus I$) such that only finitely many b_j are non-zero and assume

$$\sum_{j \in J \setminus I} b_j m_j + P \;=\; \sum_{j \in J \setminus I} b_j (m_j + P) \;=\; 0 + P$$

By definition of the quotient M/P that is $\sum_j b_j m_j \in P$ and as P is generated by A we find some $a_i \in R$ (where $i \in I$) such that only finitely many a_i are non-zero and

$$\sum_{j \in J \setminus I} b_j m_j \;=\; \sum_{i \in I} a_i m_i$$

That is $\sum_i a_i m_i + \sum_j (-b_j) m_j = 0$. But this would be a linear relation between the elements m_j (where $j \in J$) of B. But as B is a basis and hence linearly independent, this implies $a_i = 0$ for any $i \in I$ and $-b_j = 0$ for any $j \in J \setminus I$. In particular this also is the linear independence of the set $B/P := \{ m_j + P \mid j \in J \setminus I \}$.

(ii) We use the same notation $B = \{ m_j \mid j \in J \}$ and $A = \{ m_i \in i \in I \}$ as in (i), before. Let us also denote the set $A' = \{ m'_k \mid k \in I' \}$. We first prove, that $B' := (B \setminus A) \cup A'$ generates M: Consider any $x \in M$, as B generates M, there are finite subsets $I_0 \subseteq I$ and $J_0 \subseteq J \setminus I$ such that

$$x \;=\; \sum_{i \in I_0} a_i m_i + \sum_{j \in J_0} b_j m_j$$

for some a_i, $b_j \in R$. By assumption we have $m_i \in \mathrm{Lh}_R(A) = P = \mathrm{Lh}_R(A')$ such that any m_i is a

linear combination of the m'_i that is any m_i can be written in the form

$$m_i \;=\; \sum_{k\in I'} a_{i,k} m'_k$$

where of course $a_{i,k} \in R$ again and only finitely many $a_{i,k}$ are non-zero. Let us insert these equations into the equation for x and use general distributivity, to find

$$x \;=\; \sum_{k\in I'} \left(\sum_{i\in I_0} a_i a_{i,k} \right) m'_k + \sum_{j\in J_0} b_j m_j$$

That is we see, that x can be expressed as an R-linear combination over the elements m'_k (where $k \in I'$) and m_j where $j \in J_0 \subseteq J \setminus I$. As these elements belong to B' and x was arbitrary we have $\mathrm{Lh}_R(B') = M$, that is B' truly generates M. It remains to prove the R-linear independence of B': Consider a linear relation of the form

$$\sum_{j\in J\setminus I} b_j m_j + \sum_{i\in I'} a'_i m'_i \;=\; 0$$

As $P = \mathrm{Lh}_R(A) = \mathrm{Lh}_R(A')$ we turn to the quotient module M/P. Again, as for any $i \in I'$ we have $m'_i \in P$, too. Hence all the m'_i are eliminated $m'_i + P = 0 + P$ such that the sum breaks down to

$$\sum_{j\in J\setminus I} b_j m_j + \sum_{i\in I'} a'_i m'_i + P \;=\; \sum_{j\in J\setminus I} b_j \big(m_j + P\big) \;=\; 0 + P$$

But in (i) we have seen, that B/P is a basis of M/P and hence we conclude $b_j = 0$ for any $j \in J \setminus I$. Therefore in the sum above we are only left with $\sum_i a'_i m'_i = 0$. But A' was assumed to be linearly independent, too, such that we conclude $a'_i = 0$. Altogether the only linear combination of elements of B' that turns up 0 has to start with all 0 coefficients. And this is the linear independence of B'.

□

Proof of (3.63):
The direction(b) $\implies$ (a) is trivial: If $X \subseteq E^{\oplus I}$ is E-linearly independent, then for any finite subset $\{ x_1, x_2, \ldots, x_n \} \subseteq X$ and any $e_i = a_i/b_i \in E$ for which we have a relation of the form

$$e_1 x_1 + e_2 x_2 + \cdots + e_n x_n \;=\; 0$$

we necessarily hav $e_1 = e_2 = \cdots = e_n = 0$. In particular this is the case for any $e_i = a_i/1 \in R$ such that $X \subseteq R^{\oplus I}$ is R-linearly independent, as well.

Conversely for (a) $\implies$ (b): Let us again consider any $\{ x_1, x_2, \ldots, x_n \} \subseteq X$ and pick up some $a_i/b_i = e_i \in E$. That is a_i and $b_i \in R$ such that $b_i \neq 0$. Let us define (for any $j \in 1 \ldots n$)

$$b \;:=\; \prod_{i=1}^{n} b_i \quad \text{and} \quad \widehat{b}_j \;:=\; \frac{b}{b_j} \;=\; \prod_{i\neq j} b_i$$

Then b and all $\widehat{b}_j \in R$ and since R is an integral domain and all the $b_i \neq 0$ are non-zero, so are $b \neq 0$

and all $\widehat{b}_j \neq 0$. Now suppose we had a dependence relation

$$e_1x_1 + e_2x_2 + \cdots + e_nx_n \;=\; 0$$

Then multiplying this equation by b we would find another relation over R

$$0 \;=\; b\left(\sum_{i=1}^{n} e_ix_i\right) \;=\; \sum_{i=1}^{n} a_i\widehat{b}_ix_i$$

Now, since $X \subseteq R^{\oplus I}$ and hence $\{\, x_1, x_2, \ldots, x_n \,\}$ is R-linearly independent, by assumption, this means $a_i\widehat{b}_i = 0$ for any $i \in 1 \ldots n$. But as $\widehat{b}_i \neq 0$ this can only be, if $a_i = 0 \in R$ and hence $e_i = a_i/b_i = 0 \in E$. Thus we see, that X then is E-linearly independent, as well. □

Proof of (3.67):
We only have to regard the following case: M is a free R-module having the basis $\mathcal{M}$. Also at least one of R or $\mathcal{M}$ is infinite. Thereby it is clear, that the cartesian product $\mathcal{M} \times R$ also is infinite. Then we have to prove the equality of

$$|M| \;=\; \max\{\, |R|, \dim(M) \,\}$$

An $\mathcal{M}$ is a basis, we have a bijective map $\mathcal{F}_0(\mathcal{M}, R) \longleftrightarrow M$, which has already been argued for in the remark. But it also is clear, that $\mathcal{F}_0(\mathcal{M}, R)$ can be embedded into the set $\Omega(\mathcal{M} \times R)$ of finite subsets of $\mathcal{M} \times R$, that is we find an injective map of the following form

$$\mathcal{F}_0(\mathcal{M}, R) \;\hookrightarrow\; \Omega(\mathcal{M} \times R) \;:\; a \;\mapsto\; \big\{\, \big(m, a(m)\big) \mid m \in \mathcal{M},\, a(m) \neq 0 \,\big\}$$

This map is injective, as we can reconstruct a from this finite subset of $\mathcal{M} \times R$, just by filling up the rest with 0. And thereby we can use property (d) of (0.38.(v)) to find the estimate

$$|M| \;=\; |\mathcal{F}_0(\mathcal{M}, R)| \;\leq\; |\Omega(\mathcal{M} \times R)| \;=\; \max\{\, |R|, |\mathcal{M}| \,\}$$

Hereby $|\mathcal{M}| = \dim(M)$, as we assumed $\mathcal{M}$ to be an R-basis of M. But the converse inequalities are clear: As $\mathcal{M} \subseteq M$ we have $|\mathcal{M}| \leq |M|$. Also, as $\mathcal{M}$ is an R-basis of M we can choose any $m \in \mathcal{M}$, this m is linearly independent and hence $R \hookrightarrow M : a \mapsto am$ is injective. But from this we also get $|R| \leq |M|$ and hence the above equality. □

Proof of (3.68):

(i) By (3.57.(vii)) and (3.64.(i)) we may choose an S-basis A of $P \cap Q$. And by the same theorems we may extend this basis to a basis B of P, that is $A \subseteq B$ and B is an S-basis of P. Likewise we pick up an S-basis C of Q, that extends A, that is $A \subseteq C$ and C is an S-basis of Q. Let us denote $D := B \cup C$ and choose any $p \in B \cap C$ then $p \in \mathrm{Lh}(B) \cap \mathrm{Lh}(C) = P \cap Q = \mathrm{Lh}(A)$. That is there are some $(s_a) \in S^{\oplus A}$ such that

$$\sum_{a \in A} s_a a \;=\; p \;=\; \sum_{b \in B} \delta_{p,b} b \;\in\; \mathrm{Lh}(B) \;=\; P$$

And as $A \subseteq B$ both sides of the equation are linear expansions of p in terms of the basis B. Due to the uniqueness of the representation this means $p = a$ (and $s_a = 1$) for some $a \in A$ and hence

$p \in A$. That is we have proved $B \cap C = A$. Therefore D is the *disjoint* union of

$$D \;=\; A \cup (B \setminus A) \cup (C \setminus A)$$

Hence the cardinality of D is the sum of the cardinalities of A, $B \setminus A$ and $C \setminus A$ respectively. And as $A \subseteq B$ and $A \subseteq C$ this turns into

$$\begin{aligned} |D| &= |A| + |B \setminus A| + |C \setminus A| \\ &= |A| + |B| - |A| + |C| - |A| \\ &= |B| + |C| - |A| \end{aligned}$$

We will now prove, that $D = B \cup C$ is an S-basis of $P + Q$. First of all it is clear that:

$$P + Q \;=\; \mathrm{ln}(B) + \mathrm{Lh}(C) \;=\; \mathrm{Lh}(B \cup C) \;=\; \mathrm{Lh}(D)$$

That is D generates $P + Q$. Now by definition it remains to prove the linear independence of D, hence: suppose we have a linear dependence equation

$$\sum_{d \in D} x_d d \;=\; 0$$

By the above D is the disjoint union of A, $B \setminus A$ and $C \setminus A$ and hence we may split this sum into three separate parts:

$$\sum_{a \in A} x_a a + \sum_{b \in B \setminus A} x_b b + \sum_{c \in C \setminus A} x_c c \;=\; 0$$

The first way to reassemble this equation is to divide it into a part contained in $P = \mathrm{Lh}(B)$ (the left-hand side) and a part contained in $Q = \mathrm{Lh}(C)$ (the right-hand side)

$$\sum_{b \in B} x_b b \;=\; -\sum_{c \in C \setminus A} x_c c$$

Conseqently both - the left- and right-hand sides - are contained in both - P and Q. Now, as $P \cap Q = \mathrm{Lh}(A)$, there are some (uniquely determined) $(y_a) \in S^{\oplus A}$ such that

$$\sum_{b \in B} x_b b \;=\; \sum_{a \in A} y_a a$$

Again we rearrange this equation, splitting it into two parts as a basis representation of 0 within $P = \mathrm{Lh}(C)$

$$\sum_{a \in A} (x_a - y_a) a + \sum_{b \in B \setminus A} x_b b \;=\; 0$$

Now, as B is linearly independent we find $x_b = 0$ for any $b \in B \setminus A$. By precisely the same arguments we can prove that $x_c = 0$ for any $c \in C \setminus A$. So there only remains $\sum_a x_a a = 0$. Again, as A is linearly independent, this means $x_a = 0$ for any $a \in A$. Altogether we have $x_d = 0$ for any $d \in D$ and this is the linear independence of D. That is D is a S-basis of $P + Q$ and therefore we

finally got

$$\begin{aligned}\dim(P+Q) &= |D| = |B|+|C|-|A| \\ &= \dim(P)+\dim(Q)+\dim(P\cap Q)\end{aligned}$$

(ii) As in (i) above, we may choose an S-basis $A \subseteq P$ of P, as S is a skew field. Again we may extend A to an S-basis $B \subseteq V$ of V. Let us now denote $B/A := \{\, b+P \mid b \in B \setminus A \,\} \subseteq V/P$. It is easy to see, that B/A corresponds to $B \setminus A$, that is $b \mapsto b+P$ is bijective. Suppose we had $b+P = c+P$ for some $b, c \in B \setminus A$. Then $c-b \in P = \mathrm{Lh}(A)$. That is either $b = c$ or $\{\, b, c \,\} \cup A \subseteq B$ is S-linearly dependent. But as B is S-linearly independent (being a basis), the latter is absurd and hence $b = c$. This is the injectivity and the surjectivity is clear from the deinition of B/A.

We now claim that B/A is an S-basis of the quotient V/P. All we need to do is check that B/A is S-linearly independent and generates V/P. For the linear independence we suppose we had some $x_b \in S$ such that

$$0 = \sum_{b+P\in B/A} x_b(b+P) = \left(\sum_{b+P\in B/A} x_b b\right) + P = \left(\sum_{b\in B\setminus A} x_b b\right) + P$$

That is $\sum_b x_b b \in P = \mathrm{Lh}(A)$ and hence there were some $x_a \in S$ such that $\sum_b x_b b = \sum_a x_a a$. Altogether that is

$$0 = \sum_{b\in B\setminus A} x_b b - \sum_{a\in A} x_a a$$

But as $B = (B \setminus A) \cup A$ is linearly independent, this can only be if all the $x_b \in S$ and all the $x_a \in S$ are identically 0. And this is what was needed for linear inependence of B/A. Also we have to check that B/A generates V/P. To do this regard any $x+P = \in V/P$. As B is a basis of V there are some $x_b \in S$ (where $b \in B$) such that $x = \sum_b x_b b$. Again we use the split $B = (B \setminus A) \cup A$ and $A \subseteq P$ to get

$$\begin{aligned}x+P &= \left(\sum_{b\in B} x_b b\right) + P = \sum_{b\in B} x_b(b+P) \\ &= \sum_{b\in B\setminus A} x_b(b+P) = \sum_{b+P\in B/A} x_b(b+P)\end{aligned}$$

As x has been arbitrary we have $V/P = \mathrm{Lh}(B/A)$ Then as B/A is a linearly independent generating set of V/P it is a basis. And therefore

$$\dim\left(V \Big/ P\right) = |B/A| = |B\setminus A| = |B|-|A| = \dim(V)-\dim(P)$$

(iii) The dimension formula now is an easy application of (ii) and the first isomorphism theorem (3.78.(ii)) which implies, that

$$V \Big/ \mathrm{kn}(\varphi) \cong_{\mathrm{m}} \mathrm{im}(\varphi)$$

In particular we have $\dim(V/\mathrm{kn}(\varphi)) = \dim(\mathrm{im}(\varphi))$. But by (ii) we now know that $\dim(V/\mathrm{kn}(\varphi)) =$

$\dim(V) - \dim(\ker(\varphi))$ such that we truly find the claim from

$$\dim(V) - \dim(\ker(\varphi)) \;=\; \dim(\operatorname{im}(\varphi))$$

□

Proof of (3.41):
We first have to prove the equality $\mathfrak{a}R^{\oplus I} = \mathfrak{a}^{\oplus I}$. The elements of $\mathfrak{a}R^{\oplus I}$ are of the form - where $a_k \in \mathfrak{a}$ and $b_k = (b_{i,k}) \in R^{\oplus I}$

$$\sum_{k=1}^{m} a_k (b_{i,k}) \;=\; \left(\sum_{k=1}^{m} a_k b_{i,k} \right) \;\in\; \mathfrak{a}^{\oplus I}$$

That is $\mathfrak{a}R^{\oplus I} \subseteq \mathfrak{a}^{\oplus I}$, conversely consider any $a = (a_i) \in \mathfrak{a}^{\oplus I}$ and let us denote the support of a by $I_0 := \{\, i \in I \mid a_i \neq 0 \,\}$. Note that (by definition of direct sums) I_0 is a finite set. Let us also denote the canonical basis of $R^{\oplus I}$ by $\{\, e_j \mid j \in I \,\}$, that is $e_j = (\delta_{i,j}) \in R^{\oplus I}$. Then we can write

$$(a_i) \;=\; \sum_{i \in I_0} a_i \, e_i \;\in\; \mathfrak{a}R^{\oplus I}$$

Altogether we have proved $\mathfrak{a}R^{\oplus I} = \mathfrak{a}^{\oplus I}$ and it remains to prove the isomorphy of $(R/\mathfrak{a})^{\oplus I}$ and $R^{\oplus I}/\mathfrak{a}R^{\oplus I}$. To do this regard the R-linear map

$$\varphi \;:\; R^{\oplus I} \to \left(R \Big/ \mathfrak{a} \right)^{\oplus I} \;:\; (b_i) \mapsto (b_i + \mathfrak{a})$$

Clearly φ is surjective, and its kernel is given to be $\ker(\varphi) = \mathfrak{a}^I \cap R^{\oplus I} = \mathfrak{a}^{\oplus I}$ such that $\ker(\varphi) = \mathfrak{a}R^{\oplus I}$. So by the first isomorphism theorem, this induces an isomorphism of R-modules

$$\Phi \;:\; R^{\oplus I} \Big/ \mathfrak{a}R^{\oplus I} \;\xrightarrow{\sim}\; \left(R \Big/ \mathfrak{a} \right)^{\oplus I} \;:\; (b_i) + \mathfrak{a}R^{\oplus I} \mapsto (b_i + \mathfrak{a})$$

But both $R^{\oplus I}/\mathfrak{a}R^{\oplus I}$ and $(R/\mathfrak{a})^{\oplus I}$ are $(R/\mathfrak{a})$-modules and from the explict construction of Φ it is clear, that Φ even is an $(R/\mathfrak{a})$-module-homomorphism. □

Proof of (2.5):

- (a) $\implies$ (c): If $\overline{\mathfrak{a}} \trianglelefteq_{\mathrm{i}} R/\mathfrak{m}$ is an ideal, then by the correspondence theorem it is of the form $\overline{\mathfrak{a}} = \mathfrak{a}/\mathfrak{m}$ for some ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ with $\mathfrak{m} \subseteq \mathfrak{a}$. But as $\mathfrak{m}$ is maximal this means $\mathfrak{a} = \mathfrak{m}$ or $\mathfrak{a} = R$. Thus we have $\overline{\mathfrak{a}} = \{\, 0 + \mathfrak{m} \,\}$ (in the case $\mathfrak{a} = \mathfrak{m}$) or $\overline{\mathfrak{a}} = R/\mathfrak{m}$ (in the case $\mathfrak{a} = R$).

- (c) $\implies$ (b): $R/\mathfrak{m}$ is a non-zero (since $\mathfrak{m} \neq R$) commutative ring (since R is such). But it has already been shown that a commutative ring is a field if and only if it only contains the trivial ideals (viz. section 1.6).

- (b) $\implies$ (d): Let $a \notin \mathfrak{m}$, this means $a + \mathfrak{m} \neq 0 + \mathfrak{m}$. And as $R/\mathfrak{m}$ is a field there is some $b \in R$ such that $b + \mathfrak{m}$ is inverse to $a + \mathfrak{m}$. That is

$$ab + \mathfrak{m} \;=\; (a + \mathfrak{m})(b + \mathfrak{m}) \;=\; 1 + \mathfrak{m}$$

 Therefore there is some $m \in \mathfrak{m}$ such that $1 = ab + m \in aR + \mathfrak{m}$ and hence we have $aR + \mathfrak{m} = R$.

- (d) $\implies$ (a): Suppose $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$ is some ideal with $\mathfrak{m} \subseteq \mathfrak{a}$. We want to show that $\mathfrak{m}$ is maximal hence if $\mathfrak{a} = \mathfrak{m}$ then we are done. Else there is some $a \in \mathfrak{a}$ with $a \notin \mathfrak{m}$. Hence we get $aR + \mathfrak{m} = R$. But as $a \in \mathfrak{a}$ and $\mathfrak{m} \subseteq \mathfrak{a}$ we get $R = aR + \mathfrak{m} \subseteq \mathfrak{a} \subseteq R$.

□

Proof of (2.8):

- $\neg$ (a) $\implies$ $\neg$ (b): by assumption $\neg$ (a) there is some maximal ideal $\mathfrak{m} \trianglelefteq_{\mathfrak{i}} R$ such that $j \notin \mathfrak{m}$. Hence we have $\mathfrak{m} + jR = R$ such that is there is some $b \in R$ (let $a := -b$) such that $1 - aj = 1 + bj = 1 \in R^*$.

- $\neg$ (b) $\implies$ $\neg$ (a): by assumption $\neg$ (b) there is some $a \in R$ such that $1 - aj \notin R^*$. That is $(1 - aj)R \neq R$ is a non-full ideal and hence there is a maximal ideal $\mathfrak{m} \trianglelefteq_{\mathfrak{i}} R$ containing it $1 - aj \in (1 - aj)R \subseteq \mathfrak{m}$ by (2.4.(ii)). If we now had $j \in \text{JAC}(R) \subseteq \mathfrak{m}$ then also $aj \in \mathfrak{m}$ and hence we would arrive at the contradiction

$$1 \;=\; (1 - aj) + aj \;\in\; \mathfrak{m}$$

- (a) $\implies$ (b): if $j \in \mathfrak{a} \subseteq \text{JAC}(R)$ then we let $a := -1$ and as we have just proved above this yields $1 + j = 1 - aj \in R^*$ and hence (b).

- (b) $\implies$ (c): first of all we have $1 \in 1 + \mathfrak{a}$ since $0 \in \mathfrak{a}$. Now consider any $a = 1 + j$ and $b = 1 + k \in 1 + \mathfrak{a}$, that is j and $k \in \mathfrak{a}$. Then $ab = 1 + (j + k + jk) \in 1 + \mathfrak{a}$ again, as $j + k + jk \in \mathfrak{a}$. Further we get

$$(1 + j)(1 - (1 + j)^{-1}j) \;=\; (1 + j) - j \;=\; 1$$

 which implies $a^{-1} = (1 + j)^{-1} = 1 - (1 + j)^{-1}j$. And hence we also have $a^{-1} \in 1 + \mathfrak{a}$, since $-(1 + j)^{-1}j \in \mathfrak{a}$ due to $j \in \mathfrak{a}$.

- (c) $\implies$ (a): fix $j \in \mathfrak{a}$ and consider any $a \in R$. Then we also get $-aj \in \mathfrak{a}$ and hence $1 - aj \in 1 + \mathfrak{a} \subseteq R^*$ by assumption. But as we have already proved above $1 - aj \in R^*$ for any $a \in R$ means $j \in \text{JAC}(R)$.

□

Proof of (2.12):

- (a) $\implies$ (b): consider $a, b \in R$ such that $0 + \mathfrak{p} = (a + \mathfrak{p})(b + \mathfrak{p}) = ab + \mathfrak{p}$. That is $ab \in \mathfrak{p}$ and as $\mathfrak{p}$ is assumed to be prime this implies $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. This again means that $a + \mathfrak{p} = 0 + \mathfrak{p}$ or $b + \mathfrak{p} = 0 + \mathfrak{p}$ and hence $R/\mathfrak{p}$ is an integral domain. But $R/\mathfrak{p} \neq 0$ is clear, since $\mathfrak{p} \neq R$ and hence $1 + \mathfrak{p} \neq 0 + \mathfrak{p}$.

- (b) $\implies$ (c): since $R/\mathfrak{p} \neq 0$ is non-zero we have $1 + \mathfrak{p} \neq 0 + \mathfrak{p}$ or in other words $1 \notin \mathfrak{p}$ which already is (1). Now let $u, v \in R \setminus \mathfrak{p}$, then $u + \mathfrak{p} \neq 0 + \mathfrak{p}$ and $v + \mathfrak{p} \neq 0 + \mathfrak{p}$. But as $/\mathfrak{p}$ is an integral domain this then yields $uv + \mathfrak{p} = (u + \mathfrak{p})(v + \mathfrak{p}) \neq 0 + \mathfrak{p}$. Thus we also have $uv \notin \mathfrak{p}$ which is (2).

- (c) $\implies$ (a): since $1 \in R \setminus \mathfrak{p}$ we have $\mathfrak{p} \neq R$. Now consider a, $b \in R$ with $ab \in \mathfrak{p}$. Supposed we had $a \notin \mathfrak{p}$ and $b \notin \mathfrak{p}$ then a, $b \in R \setminus \mathfrak{p}$ and hence $ab \in R \setminus \mathfrak{p}$, a contradiction. Thus we truly have $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

- (a) $\implies$ (d): consider two ideals $\mathfrak{a}$, $\mathfrak{b} \trianglelefteq_{\mathrm{i}} R$ such that $\mathfrak{ab} \subseteq \mathfrak{p}$. Suppose neither $\mathfrak{a} \subseteq \mathfrak{p}$ nor $\mathfrak{b} \subseteq \mathfrak{p}$ was true. That is there would be $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ with a, $b \notin \mathfrak{p}$. Then $ab \in \mathfrak{ab} \subseteq \mathfrak{p}$. But as $\mathfrak{p}$ has is prime this yields $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, a contradiciton.

- (d) $\implies$ (a): consider a, $b \in R$ with $ab \in \mathfrak{p}$. Then we let $\mathfrak{a} := aR$ and $\mathfrak{b} := bR$. Then $\mathfrak{ab} = abR \subseteq \mathfrak{p}$ by (1.59), hence we find $a \in aR = \mathfrak{a} \subseteq \mathfrak{p}$ or $b \in bR = \mathfrak{b} \subseteq \mathfrak{p}$ by assumption. As we have also assumes $\mathfrak{p} \neq R$, this means that $\mathfrak{p}$ is prime.

□

Proof of (2.9):
Let $i \neq j \in 1 \dots r$, then $\mathfrak{m}_i \subseteq \mathfrak{m}_j$ would imply $\mathfrak{m}_i = \mathfrak{m}_j$ (since $\mathfrak{m}_i$ is maximal and $\mathfrak{m}_j \neq R$). Hence there is some $a_i \in \mathfrak{m}_i$ with $a_i \notin \mathfrak{m}_j$. And as we have just seen in (2.5) this means $a_i R + \mathfrak{m}_j = R$. But as $a_i \in \mathfrak{m}_i$ we find $R = a_i R + \mathfrak{m}_j \subseteq \mathfrak{m}_i + \mathfrak{m}_j \subseteq R$. Hence the $\mathfrak{m}_i$ are pairwise coprime. And the second claim follows from this, as we have proved in (1.61.(iv)).
Hence it remains to prove the third statement, i.e. the strict descent of the chain $\mathfrak{m}_1 \supset \mathfrak{m}_1\mathfrak{m}_2 \supset \dots \supset \mathfrak{m}_1 \dots \mathfrak{m}_k$. To do this we use induction on k (the foundation $k = 1$ is trivial), and let $\mathfrak{a} := \mathfrak{m}_1 \dots \mathfrak{m}_k$ and $\mathfrak{m} := \mathfrak{m}_{k+1}$. For any $i \in 1 \dots k$ there are $a_i \in \mathfrak{m}_i$ such that $a_i \notin \mathfrak{m}$ again. Now let $a := a_1 \dots a_k \in \mathfrak{a}$. Then $a \notin \mathfrak{m}$, as maximal ideals are prime (see the remark to (2.12) or (2.24) for a proof) and hence $a = a_1 \dots a_k \in \mathfrak{m}$ would imply $a_i \in \mathfrak{m}$ for some $i \in 1 \dots k$. In particular $a \notin \mathfrak{am} \subseteq \mathfrak{m}$, that is we have found the induction step

$$a \in (\mathfrak{m}_1 \dots \mathfrak{m}_k) \setminus (\mathfrak{m}_1 \dots \mathfrak{m}_k \mathfrak{m}_{k+1})$$

Finally we want to show that the powers $\mathfrak{m}_1^p$ and $\mathfrak{m}_2^q$ are coprime as well (the general case of $\mathfrak{m}_i$ and $\mathfrak{m}_j$ is just a reformulation of this). Suppose we had $\mathfrak{m}_1^p + \mathfrak{m}_2^q \neq R$, since R is a commutative ring (2.4.(ii)) tells us, that there is a maximal ideal $\mathfrak{m}$ containing $\mathfrak{m}_1^p + \mathfrak{m}_2^q$. That is we find the chain

$$\mathfrak{m}_1^p \subseteq \mathfrak{m}_1^p + \mathfrak{m}_2^q \subseteq \mathfrak{m}$$

in particular $\mathfrak{m}_1^p \subseteq \mathfrak{m}$. As any maximal ideal is prime we find $\mathfrak{m}_1 \subseteq \mathfrak{m}$ and hence $\mathfrak{m}_1 = \mathfrak{m}$, since $\mathfrak{m}_1$ is maximal, too. On the other hand, the same reasoning yields $\mathfrak{m}_2 = \mathfrak{m}$ which would contradict $\mathfrak{m}_1 \neq \mathfrak{m}_2$ being distinct ideals. This contradiction can only be resolved, it $\mathfrak{m}_1^p + \mathfrak{m}_2^q = R$. □

Proof of (2.18):

(i) Let $\mathfrak{b} := \bigcup \mathcal{P}$ be the union of all the prime ideals $\mathfrak{p} \in \mathcal{P}$. As $\mathcal{P}$ is a non-empty chain of ideals, (2.4) tells us, that $\mathfrak{b} \trianglelefteq_{\mathrm{i}} R$ is an ideal again, so it remains to prove that $\mathfrak{b}$ is prime. Suppose we had $\mathfrak{b} = R$, then $1 \in \mathfrak{b}$ such that $1 \in \mathfrak{p}$ for some $\mathfrak{p} \in \mathcal{P}$. But this would mean $\mathfrak{p} = R$ in contradiction to $\mathfrak{p}$ being prime. Thus $\mathfrak{b}$ is a proper ideal. Now consider a, $b \in R$ such that $ab \in \mathfrak{b}$. That is there is some $\mathfrak{p} \in \mathcal{P}$, such that $ab \in \mathfrak{p}$. As $\mathfrak{p}$ is prime, we get $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. As $\mathfrak{p} \subseteq \mathfrak{b}$ we get $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, respectively. And this means that $\mathfrak{b}$ is a prime ideal, again.

(i) Let $\mathfrak{a} := \bigcap \mathcal{P}$ be the intersection of all the prime ideals $\mathfrak{p} \in \mathcal{P}$. By (1.52) this is an ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ again, so it remains to prove that $\mathfrak{a}$ is prime. To do this consider any a, $b \in R$, such that $ab \in \mathfrak{a}$.

We need to show $a \in \mathfrak{a}$ or $b \in \mathfrak{a}$ so let's assume the opposite: $a \notin \mathfrak{a}$ and $b \notin \mathfrak{a}$. That is there must be some $\mathfrak{p} \in \mathcal{P}$ such that $a \notin \mathfrak{p}$ and some $\mathfrak{q} \in \mathcal{P}$ such that $b \notin \mathfrak{q}$. Yet $ab \in \mathfrak{a} \subseteq \mathfrak{p}$ and $\mathfrak{p}$ is prime. Then we get $b \in \mathfrak{p}$, as $a \in \mathfrak{p}$ was ruled out. Likewise we conclude $a \in \mathfrak{q}$ as $ab \in \mathfrak{q}$ but $b \notin \mathfrak{q}$. Let us summarize, by now we have

$$\begin{array}{lll} a \notin \mathfrak{p} & \text{and} & b \in \mathfrak{p} \\ a \in \mathfrak{q} & \text{and} & b \notin \mathfrak{q} \end{array}$$

If $\mathcal{P}$ was not a chain, this would be the end of the story, but as $\mathcal{P}$ is totally ordered under inclusion, we can assume $\mathfrak{p} \subseteq \mathfrak{q}$ without loss of generality. Thus we have $R \setminus \mathfrak{q} \subseteq R \setminus \mathfrak{p}$. But as $b \notin \mathfrak{p}$ we have $b \in R \setminus \mathfrak{q}$ and hence $b \in R \setminus \mathfrak{p}$, as well. But this contradicts $b \in \mathfrak{p}$ and thus we must have had $a \in \mathfrak{a}$ or $b \in \mathfrak{a}$ right from the beginning.

(ii) Clearly $\mathcal{P}$ is partially ordered under the inverse inclusion relation " $\supseteq$ " (as $\mathcal{P} \neq \emptyset$). Now let $\mathcal{O} \subseteq \mathcal{P}$ be a chain in $\mathcal{P}$, then by (i) we know that $\mathfrak{p} := \bigcap \mathcal{O} \trianglelefteq_{\mathfrak{i}} R$ is prime. Now pick any $\mathfrak{q} \in \mathcal{O}$, then as $\mathfrak{p} \subseteq \mathfrak{q}$ and the assumption on $\mathcal{P}$ we find $\mathfrak{p} \in \mathcal{P}$. Hence $\mathfrak{p}$ is a $\supseteq$-upper bound of $\mathcal{O}$. And by the lemma of Zorn this yields that $\mathcal{P}$ contains a $\supseteq$-maximal element $\mathfrak{p}_*$. But clearly $\supseteq$-maximal is $\subseteq$-minimal and hence $\mathfrak{p}_* \in \mathcal{P}_*$.

(iii) Let us take $\mathcal{Z} := \{ \mathfrak{p} \in \operatorname{Spec}(R) \mid \text{condition}(\mathfrak{p}) \}$, then $\mathcal{Z}$ is partially ordered under the inverse inclusion " $\supseteq$ " of sets. In any case $\mathcal{Z} \neq \emptyset$ is non-empty: if we imposed *none* then by assumption $R \neq 0$ and hence R has a maximal (in particular prime) ideal due to (2.4.(iv)). If we imposed $\mathfrak{p} \subseteq \mathfrak{q}$ then $\mathfrak{q} \in \mathcal{Z}$. If we imposed $\mathfrak{a} \subseteq \mathfrak{p}$ then by assumption $\mathfrak{a} \neq R$ and hence there is a maximal (in particular prime) ideal $\mathfrak{m}$ containing $\mathfrak{a} \subseteq \mathfrak{m}$ due to (2.4.(ii)) again. Finally if we supposed $\mathfrak{a} \subseteq \mathfrak{p} \subseteq \mathfrak{q}$ then we assumed $\mathfrak{a} \subseteq \mathfrak{q}$ and hence $\mathfrak{q} \in \mathcal{Z}$. Now let $\mathcal{P} \subseteq \mathcal{Z}$ be any chain in $\mathcal{Z}$ and $\mathfrak{p} := \bigcap \mathcal{P}$. Then by (i) $\mathfrak{p}$ is a prime ideal of R again. Also $\mathfrak{a} \subseteq \mathfrak{p}$ and $\mathfrak{p} \subseteq \mathfrak{q}$ are clear (if they have been imposed). Hence $\mathfrak{p} \in \mathcal{Z}$ is an upper bound of $\mathcal{P}$ (under $\supseteq$). And hence there is a maximal element $\mathfrak{p}_* \in \mathcal{Z}^*$ by the lemma of Zorn. But as $\mathfrak{p}_*$ is maximal with respect to $\supseteq$ it is minimal with respect to $\subseteq$.

(iv) By assumption $\mathfrak{a} \subseteq \mathfrak{q}$ and (iii) there is some prime ideal $\mathfrak{p}_*$ minimal among the ideals $\mathfrak{p}_* \in \{ \mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{a} \subseteq \mathfrak{p} \subseteq \mathfrak{q} \}_*$ and in particular $\mathfrak{a} \subseteq \mathfrak{p}_* \subseteq \mathfrak{q}$. It remains to prove, that $\mathfrak{p}_*$ also is a minimal element of $\{ \mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{a} \subseteq \mathfrak{p} \}$. Thus suppose we are given any prime ideal $\mathfrak{p}$ with $\mathfrak{a} \subseteq \mathfrak{p}$ and $\mathfrak{p} \subseteq \mathfrak{p}_*$. Then in particular $\mathfrak{p} \subseteq \mathfrak{q}$ and by the minimality of $\mathfrak{p}_*$ this then implies $\mathfrak{p} = \mathfrak{p}_*$. Thus $\mathfrak{p}_*$ even is minimal in this larger set.

(v) Let us take $\mathcal{Z} := \{ \mathfrak{b} \trianglelefteq_{\mathfrak{i}} R \mid \mathfrak{a} \subseteq \mathfrak{b} \subseteq R \setminus U \}$, then $\mathcal{Z}$ is partially ordered under "$\subseteq$". Clearly $\mathcal{Z} \neq \emptyset$ is non-empty, since $\mathfrak{a} \in \mathbb{Z}$, as we have assumed $\mathfrak{a} \cap U = \emptyset$. Now let $\mathcal{B} \subseteq \mathcal{Z}$ be any chain in $\mathcal{Z}$, then $\mathfrak{c} := \bigcup \mathcal{B}$ is an ideal, due to (2.4). And if we pick any $\mathfrak{b} \in \mathcal{B}$ then $\mathfrak{a} \subseteq \mathfrak{b} \subseteq \mathfrak{c}$ and hence $\mathfrak{a} \subseteq \mathfrak{c}$. And if $b \in \mathfrak{c}$ then there is some $\mathfrak{b} \in \mathcal{B} \subseteq \mathcal{Z}$ such that $b \in \mathfrak{b} \subseteq R \setminus U$. Hence we also find $\mathfrak{c} \subseteq R \setminus U$ such that $\mathfrak{c} \in \mathcal{Z}$ again. That is we have found an upper bound $\mathfrak{c}$ of $\mathcal{B}$. Hence there is a maximal element $\mathfrak{b}^* \in \mathcal{Z}$ by the lemma of Zorn. Now let $\mathfrak{p} \in \mathcal{Z}^*$ be any maximal element of $\mathcal{Z}$. As $\mathfrak{p} \subseteq R \setminus U$ and $1 \in U$ we have $1 \notin \mathfrak{p}$ such that $\mathfrak{p} \neq R$ is non-full. Now consider any $a, b \in R$ such that $ab \in \mathfrak{p}$ but suppose $a \notin \mathfrak{p}$ and $b \notin \mathfrak{p}$. As we have $\mathfrak{p} \subset \mathfrak{p} + aR$ and $\mathfrak{p} \in \mathcal{Z}^*$ is maximal we have $(\mathfrak{p} + aR) \not\subseteq R \setminus U$. That is we may choose $u \in (\mathfrak{p} + aR) \cap U$. That is $u = p + \alpha a$ for some $p \in \mathfrak{p}$ and $\alpha \in R$. Analogously we can find some $v = q + \beta b \in (\mathfrak{p} + bR) \cap U$ with $q \in \mathfrak{p}$ and

$\beta \in R$. Thereby we get

$$uv \;=\; (p+\alpha a)(q+\beta b) \;=\; pq+\alpha aq+\beta bp+\alpha\beta ab \;\in\; \mathfrak{p}$$

since p, q and $ab \in \mathfrak{p}$. But as U is multiplicatively closed and u, $v \in U$ we also have $uv \in U$. That is $uv \in \mathfrak{p} \cap U$, a contradiction to $\mathfrak{p} \in \mathcal{Z}$. Hence we have $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$ which means that $\mathfrak{p}$ is prime.

□

Proof of (2.14):

(i) We will prove the statement by induction on k - the case $k = 1$ being trivial. So let now $k \geq 2$ and let $a := a_1 \ldots a_{k-1}$ and $b := a_k$. Then $ab = a_1 \ldots a_{k-1}a_k \in \mathfrak{p}$, but as $\mathfrak{p}$ is prime this implies $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. If $b \in \mathfrak{p}$ then we are done (with $i := k$). If not then $a = a_1 \ldots a_{k-1} \in \mathfrak{p}$, so by induction hypothesis we get $a_i \in \mathfrak{p}$ for some $i \in 1 \ldots k-1$.

(ii) Analogous to (i) we prove this statement by induction on k - the case $k = 1$ being trivial again. For $k \geq 2$ we likewise let $\mathfrak{a} := \mathfrak{a}_1 \ldots \mathfrak{a}_{k-1}$ and $\mathfrak{b} := \mathfrak{a}_k$. Then $\mathfrak{ab} \subseteq \mathfrak{p}$ implies $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$ due to (2.12). If $\mathfrak{b} \subseteq \mathfrak{p}$ then we are done with $i := k$. Else $\mathfrak{a} \subseteq \mathfrak{p}$ and hence $\mathfrak{a}_i \subseteq \mathfrak{p}$ for some $i \in 1 \ldots k-1$ by induction hypothesis.

(iii) Let us choose a subset $I \subseteq 1 \ldots n$ such that $\mathfrak{a}$ is contained in the union of the $\mathfrak{b}_i$ ($i \in I$) with a minimal number of elements. That is

$$\mathfrak{a} \;\subseteq\; \bigcup_{i \in I} \mathfrak{b}_i$$

$$\forall\, J \subseteq 1 \ldots n \;:\; \mathfrak{a} \subseteq \bigcup_{i \in J} \mathfrak{b}_i \implies \#I \leq \#J$$

It is clear that this can be done, since $J = 1 \ldots n$ suffices to cover $\mathfrak{a}$ and the number of elements is a total order and hence allows to pick a minimal element. In the following we will prove that I contains precisely one element. And in this case $I = \{\, i \,\}$ we clearly have $\mathfrak{a} \subseteq \mathfrak{b}_i$ as claimed. Thus let us assume $\#I \geq 2$ and derive a contradiction: consider some fixed $j \in I$, as I has minimally many elements we have

$$\mathfrak{a} \;\not\subseteq\; \bigcup_{j \neq i \in I} \mathfrak{b}_i$$

That is there is some $a_j \in \mathfrak{a}$ such that $a_j \notin \mathfrak{b}_i$ for any $j \neq i \in I$. In particular we find $a_j \in \mathfrak{b}_j$, as the $\mathfrak{b}_i$ ($i \in I$) cover $\mathfrak{a}$. Let us pick one such a_j for every $j \in I$. If $\#I = 2$ then we may assume $I = \{\, 1, 2 \,\}$ without loss of generality. As a_1 and $a_2 \in \mathfrak{a}$ we also have $a_1 + a_2 \in \mathfrak{a}$. Suppose we had $a_1 + a_2 \in \mathfrak{b}_1$ then $a_2 = (a_1 + a_2) + (-a_1) \in \mathfrak{b}_1$ as well, a contradiction. Likewise we find that $a_1 + a_2 \notin \mathfrak{b}_2$. But now $a_1 + a_2 \in \mathfrak{a} \subseteq \mathfrak{b}_1 \cup \mathfrak{b}_2$ provides a contradiction. Hence $\#I = 2$ cannot be. Now assume $\#I \geq 3$, then by assumption there is some $k \in I$ such that $\mathfrak{b}_k$ is prime. Without loss of generality (that is by renumbering) we may assume $I = 1 \ldots m$ and $\mathfrak{b}_1$ to be prime. As any $a_i \in \mathfrak{a}$ we also have $a_1 + a_2 \ldots a_m \in \mathfrak{a}$. Suppose $a_1 + a_2 \ldots a_m \in \mathfrak{b}_i$ for some $i \in 2 \ldots m$, then $a_1 = (a_1 + a_2 \ldots a_m) + (-a_2 \ldots a_m) \in \mathfrak{b}_i$ too, a contradiction. And if we suppose $a_1 + a_2 \ldots a_m \in \mathfrak{b}_1$ then $a_2 \ldots a_m = (a_1 + a_2 \ldots a_m) + (-a_1) \in \mathfrak{b}_1$ too. As $\mathfrak{b}_1$ is prime we find $a_i \in \mathfrak{b}_1$ for some $i \in 2 \ldots m$ due to (i). But this is a contradiction, altogether $a_1 + a_2 \ldots a_m$ is

contained in $\mathfrak{a}$ but none of the $\mathfrak{b}_i$ for $i \in I$, a contradiction. Hence the assumption $\#I \geq 3$ has to be abandoned, which only leaves $\#I = 1$.

(iv) For the implication (a) $\implies$ (b) we first note that by definition of the minimal spectrum we have $\mathrm{Smin}R \subseteq \mathrm{Spec}(R)$ and by assumption also $\mathrm{Spec}(R) = \mathrm{Smax}(R)$ such that $\mathrm{Smin}(R) \subseteq \mathrm{Smax}(R)$. For the converse inclusion we regard any maximal ideal $\mathfrak{m} \trianglelefteq_{\mathrm{i}} R$. In particular $\mathfrak{m}$ is prime, now take $\mathfrak{a} = 0$ to impose no restrictions in (2.18.(iv)) to produce a minimal ideal $\mathfrak{p}_* \in \mathrm{Smin}(R)$ such that $\mathfrak{p}_* \subseteq \mathfrak{m}$. In particular $\mathfrak{p}_*$ is prime and hence maximal by assumption. But now $\mathfrak{p}_* \subseteq \mathfrak{m} \neq R$ implies $\mathfrak{p}_* = \mathfrak{m}$, such that $\mathfrak{m}$ is a minimal prime ideal of R. Therefore $\mathrm{Smax}(R) \subseteq \mathrm{Smin}(R)$, as well.

For the implication (b) $\implies$ (a) we only have to show $\mathrm{Spec}(R) \subseteq \mathrm{Smax}(R)$. That is we begin with any $\mathfrak{p} \in \mathrm{Spec}(R)$. Again take $\mathfrak{a} = 0$ and use (2.18.(iv)) to find a minimal prime ideal $\mathfrak{p}_* \in \mathrm{Smin}(R)$ such that $\mathfrak{p}_* \subseteq \mathfrak{p}$. By assumption $\mathfrak{p}_*$ is maximal, such that $\mathfrak{p}_* = \mathfrak{p}$. In particular $\mathfrak{p} = \mathfrak{p}_* \in \mathrm{Smin}(R) = \mathrm{Smax}(R)$ is a maximal ideal.

And by definition of the Krull-dimension we have $\mathrm{kdim}(R) = 0$ if and only if any chain of prime ideals has length 1. That is any $\mathfrak{p} \in \mathrm{Spec}(R)$ admits no distinct prime ideals below or above it. And this is precisely the case if $\mathfrak{p}$ is both: maximal and minimal. Hence $\mathrm{kdim}(R) = 0$ is just a reformulation of property (b) in other words.

□

Proof of (2.10):
As the maximal ideals $\mathfrak{m}_i$ are distinct, we know by (2.9) that $\mathfrak{m}_i + \mathfrak{m}_j = R$ are coprime. Hence we may employ the Chinese remainder theorem (1.99.(iii)) to get the isomorphism

$$R \Big/ \mathfrak{j} \;\cong_{\mathrm{r}}\; \bigoplus_{i=1}^{r} R \Big/ \mathfrak{m}_i \;:\; a + \mathfrak{j} \mapsto \Big(a + \mathfrak{m}_i\Big)$$

Now consider any prime ideal $\overline{\mathfrak{p}} \trianglelefteq_{\mathrm{i}} R/\mathfrak{j}$, then by the correspondence theorem of ideals (1.66) $\overline{\mathfrak{p}}$ is of the form $\overline{\mathfrak{p}} = \mathfrak{p}/\mathfrak{j}$ for some prime ideal $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ of R, with $\mathfrak{j} \subseteq \mathfrak{p}$. However by (2.9) we also know that $\mathfrak{j}$ is the product $\mathfrak{j} = \mathfrak{m}_1 \cdot \mathfrak{m}_2 \cdot \dots \cdot \mathfrak{m}_r$ of these maximal ideals. And as $\mathfrak{p}$ is prime $\mathfrak{m}_1 \dots \mathfrak{m}_r \subseteq \mathfrak{p}$ implies $\mathfrak{m}_i \subseteq \mathfrak{p}$ for some $i \in 1 \dots r$ - this is (2.14.(ii)). But as $\mathfrak{m}_i$ is maximal, $\mathfrak{m}_i \subseteq \mathfrak{p} \neq R$ implies $\mathfrak{m}_i = \mathfrak{p}$ and hence $\overline{\mathfrak{p}} = \mathfrak{m}_i/\mathfrak{j}$. In particular any prime ideal $\overline{\mathfrak{p}}$ already is a maximal ideal. □

Proof of (2.16):
As any ideal $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ contains $0 \in \mathfrak{p}$ we have $0 \subseteq \mathfrak{p}$ such that $\mathbb{V}(0) = \mathrm{Spec}(R)$. And as any prime ideal $\mathfrak{p} \in \mathrm{Spec}(R)$ is proper $\mathfrak{p} \neq R$ we *never* have $R \subseteq \mathfrak{p}$. That is $\mathbb{V}(R) = \emptyset$. We will now prove

$$\mathbb{V}\left(\sum_{i \in I} \mathfrak{a}_i\right) \;=\; \bigcap_{i \in I} \mathbb{V}(\mathfrak{a}_i)$$

Clearly if $\sum_i \mathfrak{a}_i \subseteq \mathfrak{p}$ then $\mathfrak{a}_i \subseteq \mathfrak{p}$ for any $i \in I$ and hence $\mathfrak{p} \in \mathbb{V}(\mathfrak{a}_i)$ for any $i \in I$. Conversely let $\mathfrak{a}_i \subseteq \mathfrak{p}$ for any $i \in I$. If $b \in \mathfrak{b} := \sum_i \mathfrak{a}_i$ then there is a finite subset $\Omega \subseteq I$ and $a_i \in \mathfrak{a}_i$ (where $i \in \Omega$) such that $b = \sum_i a_i$ (where the sum runs over $i \in \Omega$). In particular $a_i \in \mathfrak{a}_i \subseteq \mathfrak{p}$ and hence $b \in \mathfrak{p}$ such

that $\mathfrak{b} \subseteq \mathfrak{p}$ which in turn is $\mathfrak{p} \in \mathbb{V}(\mathfrak{b})$. It remains to prove

$$\mathbb{V}\left(\bigcap_{i=1}^{n} \mathfrak{a}_i\right) \;=\; \bigcup_{i=1}^{n} \mathbb{V}(\mathfrak{a}_i)$$

If $\bigcap_i \mathfrak{a}_i \subseteq \mathfrak{p}$ then - as $\mathfrak{p}$ is prime and we know (2.14.(ii)) - then there is some $j \in 1 \ldots n$ such that $\mathfrak{a}_j \subseteq \mathfrak{p}$. But this again means $\mathfrak{p} \in \mathbb{V}(\mathfrak{a}_j)$ for some $j \in 1 \ldots n$. Conversely if $\mathfrak{p} \in \mathbb{V}(\mathfrak{a}_j)$ for some $j \in 1 \ldots n$ then $\bigcap_i \mathfrak{a}_i \subseteq \mathfrak{a}_j \subseteq \mathfrak{p}$ such that $\mathfrak{p} \in \mathbb{V}(\bigcap_i \mathfrak{a}_i)$ is granted.

It remains to prove $\mathbb{V}(abR) = \mathbb{V}(aR) \cup \mathbb{V}(bR)$: As $ab \in aR$ we have $abR \subseteq aR$ and from this it is clear, that $\mathbb{V}(aR) \subseteq \mathbb{V}(abR)$. As the same is true for $\mathbb{V}(bR) \subseteq \mathbb{V}(abR)$ we have the inclusion $\mathbb{V}(aR) \cup \mathbb{V}(bR) \subseteq \mathbb{V}(abR)$. For the converse inclusion we regard any $\mathfrak{p} \in \mathbb{V}(abR)$, that is $ab \in abR \subseteq \mathfrak{p}$. As $\mathfrak{p}$ is a prime ideal and $ab \in \mathfrak{p}$ we conclude $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. In case $a \in \mathfrak{p}$ we have $aR \subseteq \mathfrak{p}$, which is $\mathfrak{p} \in \mathbb{V}(aR)$. Likewise we conclude $\mathfrak{p} \in \mathbb{V}(bR)$ from $b \in \mathfrak{p}$. In any case we have $\mathfrak{p} \in \mathbb{V}(aR) \cup \mathbb{V}(bR)$ and as this is true for any $\mathfrak{p} \in \mathbb{V}(abR)$, this means $\mathbb{V}(abR) \subseteq \mathbb{V}(aR) \cup \mathbb{V}(bR)$, too. □

Proof of (2.17):

- We will first show the well-definedness of $\mathrm{Spec}(\varphi)$ - it is clear that $\varphi^{-1}(\mathfrak{q}) = \{\, a \in R \mid \varphi(a) \in \mathfrak{q} \,\}$ is an ideal in R. Thus it only remains to show that $\varphi^{-1}(\mathfrak{q}) \in X$ truly is prime. First of all $\varphi^{-1}(\mathfrak{q}) \neq R$ as else $1 \in \varphi^{-1}(\mathfrak{q})$ and this would mean $1 = \varphi(1) \in \mathfrak{q}$. But this is absurd, as $\mathfrak{q}$ is prime and hence $\mathfrak{q} \neq S$. Hence we consider $ab \in \varphi^{-1}(\mathfrak{q})$, i.e. $\varphi(ab) = \varphi(a)\varphi(b) \in \mathfrak{q}$. As $\mathfrak{q} \in Y$ is prime, this yields $\varphi(a) \in \mathfrak{q}$ or $\varphi(b) \in \mathfrak{q}$, that is $a \in \varphi^{-1}(\mathfrak{q})$ or $b \in \varphi^{-1}(\mathfrak{q})$ again.

- Next we will show that for any $a \in R$ we have $(\mathrm{Spec}\varphi)^{-1}(X_a) = Y_{\varphi(a)}$. But this is immediate from elementary set theory, since

$$(\mathrm{Spec}(\varphi))^{-1}(X_a) \;=\; \left\{\, \mathfrak{q} \in Y \mid a \notin \varphi^{-1}(\mathfrak{q}) \,\right\} \;=\; Y_{\varphi(a)}$$

- Likewise $(\mathrm{Spec}(\varphi))(\mathbb{V}(\mathfrak{b})) \subseteq \mathbb{V}(\varphi^{-1}(\mathfrak{b}))$ is completely obvious, once we translate these sets back into set-theory, then we have to show

$$\left\{\, \varphi^{-1}(\mathfrak{q}) \mid \mathfrak{b} \subseteq \mathfrak{q} \in Y \,\right\} \;\subseteq\; \left\{\, \mathfrak{p} \in X \mid \varphi^{-1}(\mathfrak{b}) \subseteq \mathfrak{p} \,\right\}$$

 Thus we have to show that $\mathfrak{b} \subseteq \mathfrak{q} \in Y$ implies $\varphi^{-1}(\mathfrak{b}) \subseteq \varphi^{-1}(\mathfrak{q}) \in X$. But $\mathfrak{b} \subseteq \mathfrak{q}$ clearly implies $\varphi^{-1}(\mathfrak{b}) \subseteq \varphi^{-1}(\mathfrak{q})$ and we have just proved, that $\varphi^{-1}(\mathfrak{q}) \in X$ as well.

- Finally it remains to prove $(\mathrm{Spec}(\varphi))^{-1}(\mathbb{V}(\mathfrak{a})) = \mathbb{V}(\langle \varphi(\mathfrak{a}) \rangle_i)$. So let us first translate the claim back into elementary set-theory again

$$\left\{\, \mathfrak{q} \in Y \mid \mathfrak{a} \subseteq \varphi^{-1}(\mathfrak{q}) \,\right\} \;=\; \{\, \mathfrak{q} \in Y \mid \varphi(\mathfrak{a}) \subseteq \mathfrak{q} \,\}$$

 But by definition we have $\varphi^{-1}(\mathfrak{q}) = \{\, a \in R \mid \varphi(a) \in \mathfrak{q} \,\}$, and hence the inclusion $\mathfrak{a} \subseteq \varphi^{-1}(\mathfrak{q})$ trivially implies $\varphi(\mathfrak{a}) \subseteq \mathfrak{q}$ and vice versa.

□

Proof of (2.22):

(i) First of all $\mathfrak{a} \subseteq \mathfrak{a} : b$, because if $a \in \mathfrak{a}$ then also $ab \in \mathfrak{a}$, as $\mathfrak{a}$ is an ideal. Next we will prove that $\mathfrak{a} : b \trianglelefteq_{\mathrm{i}} R$ is an ideal of R. It is clear that $0 \in \mathfrak{a} : b$ since $0b = 0 \in \mathfrak{a}$. Let now p and $q \in \mathfrak{a} : b$, that is pb and $qb \in \mathfrak{a}$. Then $(p+q)b = pb + qb \in \mathfrak{a}$, $(-p)b = (-pb) \in \mathfrak{a}$ and for any $a \in R$ we also get $(ap)b = a(pb) \in \mathfrak{a}$ which means $p+q$, $-p$ and $ap \in \mathfrak{a} : b$ respectively.

(ii) First of all $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$, because if $a \in \mathfrak{a}$ then for $k = 1$ we get $a^k = a \in \mathfrak{a}$. Next we will prove that $\sqrt{\mathfrak{a}} \trianglelefteq_{\mathrm{i}} R$ is an ideal. It is clear that $0 \in \mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$. Now let a and $b \in \sqrt{\mathfrak{a}}$ that is $a^k \in \mathfrak{a}$ and $b^l \in \mathfrak{a}$ for some $k, l \in \mathbb{N}$. Then we get

$$\begin{aligned}
(-a)^k &= (-1)^k a^k \\
(ab)^l &= a^l b^l \\
(a+b)^{k+l} &= \sum_{i=0}^{k+l} \binom{k+l}{i} a^i b^{k+l-i} \\
&= \sum_{i=0}^{k} \binom{k+l}{i} a^i b^{k+l-i} + \sum_{i=k+1}^{k+l} \binom{k+l}{i} a^i b^{k+l-i} \\
&= \sum_{i=0}^{k} \binom{k+l}{i} a^i b^{k+l-i} + \sum_{j=1}^{l} \binom{k+l}{k+j} a^{k+j} b^{l-j} \\
&= \left(\sum_{i=0}^{k} \binom{k+l}{i} a^i b^{k-i} \right) b^l + \left(\sum_{j=1}^{l} \binom{k+l}{k+j} a^j b^{l-j} \right) a^k
\end{aligned}$$

As all these elements are contained in $\mathfrak{a}$ again, we again found $a+b$, $-a$ and $ab \in \sqrt{\mathfrak{a}}$. Thus it remains to prove that $\sqrt{\mathfrak{a}}$ is a radical ideal. Thus let $a \in R$ be contained in the radical of $\sqrt{\mathfrak{a}}$, that is $a^k \in \sqrt{\mathfrak{a}}$ for some $k \in \mathbb{N}$. And hence there is some $l \in \mathbb{N}$ such that $a^{kl} = (a^k)^l \in \mathfrak{a}$. But this already means $a \in \sqrt{\mathfrak{a}}$ and the converse inclusion is clear.

(iii) If $a \in \mathfrak{a} : b$ then $ab \in \mathfrak{a} \subseteq \mathfrak{b}$ and hence $a \in \mathfrak{b} : b$ again. Likewise if we are given $a \in \sqrt{\mathfrak{a}}$ then there is some $k \in \mathbb{N}$ such that $a^k \in \mathfrak{a} \subseteq \mathfrak{b}$ and hence $a \in \sqrt{\mathfrak{b}}$ already.

(iv) If $1 \in R = \mathfrak{a} : b$ then $b = 1b \in \mathfrak{a}$. And if $b \in \mathfrak{a}$ then for any $a \in R$ we have $ab \in \mathfrak{a}$, since $\mathfrak{a}$ is an ideal. But this also means $\mathfrak{a} : b = R$. Now let $\mathfrak{p}$ be a prime ideal of R, if $b \in \mathfrak{p}$ then we have alredy seen $\mathfrak{p} : b = R$. Thus assume $b \notin \mathfrak{p}$. Then $a \in \mathfrak{p} : b$ is equivalent to $ab \in \mathfrak{p}$ for any $a \in R$. But as $\mathfrak{p}$ is prime this implies $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. The latter is untrue by assumption so we get $a \in \mathfrak{p}$. That is we have proved $\mathfrak{p} : b \subseteq \mathfrak{p}$ and the converse inclusion has been proved in (i) generally.

(v) If $\emptyset \neq \mathcal{A} \subseteq \operatorname{Srad}(R) \subseteq \operatorname{Ideal}(R)$, then the intersection $\bigcap \mathcal{A} \trianglelefteq_{\mathrm{i}} R$ already is an ideal of R due to (1.52). Thus it remains to show that $\bigcap \mathcal{A}$ is radical. Let $a^k \in \bigcap \mathcal{A}$, that is $a^k \in \mathfrak{a}$ for any $\mathfrak{a} \in \mathcal{A}$. But as $\mathfrak{a}$ is radical we find that $a \in \mathfrak{a}$. As this is true for any $\mathfrak{a} \in \mathcal{A}$ we found $a \in \bigcap \mathcal{A}$.

(v) Consider any $a \in R$, then a is contained in the intersection of all $\mathfrak{a}_i : \mathfrak{b}$ iff $a \in \mathfrak{a}_i : b$ for any $i \in I$. And this again is equivalent to $ab \in \mathfrak{a}_i$ for any $i \in I$. Thus we have already found the equivalence

$$a \in \bigcap_{i \in I} (\mathfrak{a}_i : b) \iff ab \in \bigcap_{i \in I} \mathfrak{a}_i \iff a \in \left(\bigcap_{i \in I} \mathfrak{a}_i \right) : b$$

□

Proof of (2.23):
(c) $\iff$ (a) is trivial and so is (a) $\implies$ (b). For the converse implication it suffices to remark, that $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$ is true for any ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ (as $a \in \mathfrak{a}$ implies $a = a^1 \in \mathfrak{a}$). Thus we prove (a) $\implies$ (d): Let $b + \mathfrak{a}$ be a nilpotent of $R/\mathfrak{a}$, that is $b^k + \mathfrak{a} = (b + \mathfrak{a})^k = 0 + \mathfrak{a}$ for some $k \in \mathbb{N}$. This means $b^k \in \mathfrak{a}$ and hence $b \in \sqrt{\mathfrak{a}} \subseteq \mathfrak{a}$ by assumption. And from $b \in \mathfrak{a}$ we find $b + \mathfrak{a} = 0 + \mathfrak{a}$. Conversely (d) $\implies$ (c): consider any $b \in R$ such that $b^k \in \mathfrak{a}$. Then $(b + \mathfrak{a})^k = b^k + \mathfrak{a} = 0 + \mathfrak{a}$ and hence $b + \mathfrak{a}$ is a nilpotent of $R/\mathfrak{a}$. By assumption this means $b + \mathfrak{a} = 0 + \mathfrak{a}$ or in other words $b \in \mathfrak{a}$. □

Proof of (2.24):
The equivalences of the respecive properties of the ideal and its quotient ring have been shown in (2.5), (2.12) and (2.23) respectively. Hence if $\mathfrak{m} \trianglelefteq_{\mathrm{i}} R$ is maximal then $R/\mathfrak{m}$ is a field. In particular $R/\mathfrak{m}$ is a non-zero integral domain which means that $\mathfrak{m}$ is prime. And if $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ is prime, then $R/\mathfrak{p}$ is an integral domain and hence reduced which again means that $\mathfrak{p}$ is a radical ideal. Yet we also wish to present a direct proof of this:

- $\mathfrak{m}$ maximal $\implies$ $\mathfrak{m}$ prime: consider $a, b \in \mathfrak{m}$ with $ab \in \mathfrak{m}$, but suppose $a \notin \mathfrak{m}$ and $b \notin \mathfrak{m}$. This means $\mathfrak{m} \subset \mathfrak{m} + aR$ and hence $\mathfrak{m} + aR = R$, as $\mathfrak{m}$ is maximal. Hence there are $m \in \mathfrak{m}$ and $\alpha \in R$ such that $m + \alpha a = 1$. Likewise there are $n \in \mathfrak{m}$ and $\beta \in R$ such that $n + \beta b = 1$. Thereby

$$1 \;=\; (m + \alpha a)(n + \beta b) \;=\; mn + \alpha an + \beta bm + \alpha\beta ab$$

 But as m, n and $ab \in \mathfrak{m}$ we hence found $1 \in \mathfrak{m}$ which means $\mathfrak{m} = R$. But this contradicts $\mathfrak{m}$ being maximal.

- $\mathfrak{p}$ prime $\implies$ $\mathfrak{p}$ radical: consider $a \in R$ with $a^k \in \mathfrak{p}$. As $\mathfrak{p}$ is prime we have $k \geq 0$ (as else $1 = a^0 \in \mathfrak{p}$ such that $\mathfrak{p} = R$). But $\mathfrak{p}$ is prime and hence $a^k \in \mathfrak{p}$ for some $k \geq 1$ implies $a \in \mathfrak{p}$ due to (2.14.(i)). This means that $\mathfrak{p}$ is radical, due to (2.23.(c)).

□

Proof of (2.25):

(i) As $\mathfrak{a} \neq R$ is proper, there is a maximal ideal containing $\mathfrak{a}$ and maximal ideals are prime. Hence $\mathbb{V}(\mathfrak{a}) = \{\, \mathfrak{p} \mid \mathfrak{a} \subseteq \mathfrak{p} \,\}$ is non-empty, such that the intersection is well-defined. We have to prove $\sqrt{\mathfrak{a}} = \bigcap \mathbb{V}(\mathfrak{a})$. Thereby the inclusion "$\subseteq$" is clear, as any $\mathfrak{p}$ that contains $\mathfrak{a}$ also contains $\sqrt{\mathfrak{a}}$. For the converse inclusion we are given some $a \in R$ such that $a \in \mathfrak{p}$ for any prime ideal $\mathfrak{p} \in \mathbb{V}(\mathfrak{a})$. Now let $U := \{\, 1, a, a^2 \ldots \}$, then it is clear that U is multiplicatively closed. Suppose $\mathfrak{a} \cap U = \emptyset$, then by (2.18.(iv)) there was an ideal $\mathfrak{b} \trianglelefteq_{\mathrm{i}} R$ maximal with $\mathfrak{a} \subseteq \mathfrak{b} \subseteq R \setminus U$. And this ideal $\mathfrak{b}$ was prime. But as $\mathfrak{b} \cap U = \emptyset$ and $a \in U$ we have $a \notin \mathfrak{b}$ even though $\mathfrak{b} \in \mathbb{V}(\mathfrak{a})$, a contradiction. Thus we have $\mathfrak{a} \cap U \neq \emptyset$, that is there is some $b \in U$ such that $b \in \mathfrak{a}$. By construction of U b is of the form $b = a^k$ for some $k \in \mathbb{N}$. And this means $a \in \sqrt{\mathfrak{a}}$.

(i) Let us denote $\mathbb{V}(\mathfrak{a}) := \{\, \mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{a} \subseteq \mathfrak{p} \,\}$ again and $\mathcal{M} := \mathbb{V}(\mathfrak{a})_*$. Then in (i) above we have just seen the identity

$$\sqrt{\mathfrak{a}} \;=\; \bigcap \mathbb{V}(\mathfrak{a})$$

We now have to prove $\bigcap \mathbb{V}(\mathfrak{a}) = \bigcap \mathcal{M}$. As $\mathcal{M} \subseteq \mathbb{V}(\mathfrak{a})$ the inclusion "$\subseteq$" is clear. For the converse inclusion we are given any $a \in \bigcap \mathcal{M}$ and any $\mathfrak{q} \in \mathbb{V}(\mathfrak{a})$ and need to show $a \in \mathfrak{q}$. But as $\mathfrak{a} \subseteq \mathfrak{q}$

by (i) there is some $\mathfrak{p}_* \in \mathcal{M}$ such that $\mathfrak{a} \subseteq \mathfrak{p}_* \subseteq \mathfrak{p}$. And as $a \in \bigcap \mathcal{M}$ we find $a \in \mathfrak{p}_*$ and hence $a \in \mathfrak{q}$. Thus we have also established inclusion " $\supseteq$ ".

(ii) By definition it is clear that $\text{NIL}(R) = \sqrt{0}$ is the radical of the zero-ideal. And the further equalities given are immediate from (ii) above.

(iii) Let $a \in R$ be contained in the radical of $\sqrt{\mathfrak{a}}$, that is $a^k \in \sqrt{\mathfrak{a}}$ for some $k \in \mathbb{N}$. And hence there is some $l \in \mathbb{N}$ such that $a^{kl} = (a^k)^l \in \mathfrak{a}$. But this already means $a \in \sqrt{\mathfrak{a}}$ and the converse inclusion is clear.

(v) As $\mathfrak{a}\,\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$ we have $\sqrt{\mathfrak{a}\,\mathfrak{b}} \subseteq \sqrt{\mathfrak{a} \cap \mathfrak{b}}$ by (i). Next let $a \in \sqrt{\mathfrak{a} \cap \mathfrak{b}}$, that is there is some $k \in \mathbb{N}$ such that $a^k \in \mathfrak{a} \cap \mathfrak{b}$. Now $a^k \in \mathfrak{a}$ and $a^k \in \mathfrak{b}$ implies $a \in \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$. Finally consider some $a \in \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$, that is $a^i \in \mathfrak{a}$ and $a^j \in \mathfrak{b}$ for some $i, j \in \mathbb{N}$. Then $a^{i+j} = a^i a^j \in \mathfrak{a}\,\mathfrak{b}$ and hence $a \in \sqrt{\mathfrak{a}\,\mathfrak{b}}$. Altogether we have proved the following chain of inclusions

$$\sqrt{\mathfrak{a}\,\mathfrak{b}} \;\subseteq\; \sqrt{\mathfrak{a} \cap \mathfrak{b}} \;\subseteq\; \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}} \;\subseteq\; \sqrt{\mathfrak{a}\,\mathfrak{b}}$$

(vi) By induction on (v) we know that $\sqrt{\mathfrak{a}^n} = \sqrt{\mathfrak{a}} \cap \cdots \cap \sqrt{\mathfrak{a}}$ (n-times). And this obviously equals $\sqrt{\mathfrak{a}}$ such that we get the equality $\sqrt{\mathfrak{a}^n} = \sqrt{\mathfrak{a}}$ claimed. And if $\mathfrak{a}$ is a radical ideal, to begin with, then $\sqrt{\mathfrak{a}^k} = \sqrt{\mathfrak{a}} = \mathfrak{a}$ again.

(iv) In a first step let us assume $k = 1$, that is $\mathfrak{a} \subseteq \mathfrak{p} \subseteq \sqrt{\mathfrak{a}}$, then in particular we have $\mathfrak{a} \subseteq \mathfrak{p}$ and hence $\sqrt{\mathfrak{a}} \subseteq \sqrt{\mathfrak{p}}$. Yet as $\mathfrak{p}$ is prime we also have $\sqrt{\mathfrak{p}} = \mathfrak{p}$ due to (2.24). Thereby we get $\sqrt{\mathfrak{a}} \subseteq \mathfrak{p} \subseteq \sqrt{\mathfrak{a}}$ by assumption. Now consider an arbitrary $k \in \mathbb{N}$. Then by (vi) we have $\mathfrak{a}^k \subseteq \mathfrak{p} \subseteq \sqrt{\mathfrak{a}} = \sqrt{\mathfrak{a}^k}$. Thus by the case $k = 1$ (using $\mathfrak{a}^k$ instead of $\mathfrak{a}$) we get $\mathfrak{p} = \sqrt{\mathfrak{a}^k} = \sqrt{\mathfrak{a}}$, the latter by (vi) again.

(vii) By assumption $\mathfrak{a}$ is finitely generated, that is there are $a_i \in R$ such that $\mathfrak{a} = \langle a_1, \ldots, a_n \rangle_{\text{i}}$. And as $\mathfrak{a}$ is contained in the radical of $\mathfrak{b}$ we find that for any $i \in 1 \ldots n$ there is some $k(i) \in \mathbb{N}$ such that $a_i^{k(i)} \in \mathfrak{b}$. Now let $k := k(1) + \cdots + k(n)$ and consider $f_1, \ldots, f_k \in \mathfrak{a}$. That is

$$f_j \;=\; \sum_{i=1}^{n} f_{i,j} a_i$$

for some $f_{i,j} \in R$. Using (1.41) we now extract the product of the f_j

$$\prod_{j=1}^{k} f_j \;=\; \prod_{j=1}^{k} \sum_{i=1}^{n} f_{i,j} a_i \;=\; \sum_{i \in I} \prod_{j=1}^{k} f_{i_j,j} a_{i_j}$$

where $I = (1 \ldots n)^k$ and $i = (i_1, \ldots, i_k) \in I$. For any $h \in 1 \ldots n$ we now let $m(h) := \#\left\{ j \in 1 \ldots k \mid i_j = h \right\}$ the number of times h appears in the collection of i_j. Then it is clear that $m(1) + \cdots + m(n) = k = k(1) + \cdots + k(n)$ Hence there has to be some index $h \in 1 \ldots n$ such that $k(h) \leq m(h)$. Thereby $a_h^{m(h)}$ divides $a_h^{k(h)} \in \mathfrak{b}$ such that

$$b_i \;:=\; \prod_{j=1}^{k} a_{i_j} \;=\; \prod_{h=1}^{n} a_h^{m(h)} \;\in\; \mathfrak{b}$$

This now can be used to show $f_1 \dots f_k \in \mathfrak{b}$. Simply rearrange to find

$$\prod_{j=1}^{k} f_j \;=\; \sum_{i\in I}\prod_{j=1}^{k} f_{i_j,j}a_{i_j} \;=\; \sum_{i\in I}\left(\prod_{j=1}^{k} f_{i_j,j}\right) b_i \;\in\; \mathfrak{b}$$

Now recall that - by definition - $\mathfrak{a}^k$ consists precisely of sums of elements of the form $f_1 \dots f_k$ where $f_j \in \mathfrak{a}$. As we have seen any such element is contained in $\mathfrak{b}$ and hence $\mathfrak{a}^k \subseteq \mathfrak{b}$.

(viii) If a is contained in the radical of the intersection of the $\mathfrak{a}_i$ then there is some $k \in \mathbb{N}$ such that a is contained in the intersection of the $\mathfrak{a}_i$. That is $a^k \in \mathfrak{a}_i$ for any $i \in I$ and hence $a \in \sqrt{\mathfrak{a}_i}$ for any $i \in I$.

(viii) Let a be contained in the sum of the radicals $\sqrt{\mathfrak{a}_i}$. That is a is a finite sum of the form $a = a_1 + + \dots a_n$ where a_j is contained in the radical of $\mathfrak{a}_{i(j)}$. Thereby for any $j \in 1 \dots n$ we get

$$a_j \in \sqrt{\mathfrak{a}_{i(j)}} \quad\Longrightarrow\quad \exists\, k(j) \in \mathbb{N} \;:\; a_j^{k(j)} \in \mathfrak{a}_{i(j)}$$

Now let $k := k(1) + \dots + k(n) \in \mathbb{N}$, then by the polynomial rule (1.41)

$$a^k \;=\; \sum_{|\alpha|=k}\prod_{j=1}^{n} a_j^{\alpha(j)}$$

Suppose that for any $j \in 1 \dots n$ we had $\alpha(j) = k(j)$, then $|\alpha| = \alpha(1) + \dots + \alpha(n) < k(1) + \dots + k(n) = k$, a contradiction. Hence there is some $j \in 1 \dots n$ such that $k(j) \leq \alpha(j)$. And for this j we have $a_j^{\alpha(j)} \in \mathfrak{a}_{i(j)}$. Thus a^k is contained in the radical of $\mathfrak{a}_{i(1)} + \dots + \mathfrak{a}_{i(n)}$ and in particular in the radical of the sum of all $\mathfrak{a}_i$.

□

Proof of (2.28):
Fix any commutative ring $(E, +, \cdot)$ and consider the polynomial ring $S := E[t_i \mid 1 \leq i \in \mathbb{N}]$ in countable infinitely many variables over E. Then we take to the quotient where for any $1 \leq i \in \mathbb{N}$ we have $t_i^i = 0$. Formally

$$R \;:=\; {}^{S}\!\Big/_{\mathfrak{v}} \quad\text{where}\quad \mathfrak{v} \;:=\; \langle t_i^i \mid 1 \leq i \in \mathbb{N}\rangle_{\mathfrak{i}}$$

For any $f \in S$ let us denote its residue class in R by $\overline{f} := f + \mathfrak{v}$. And further let us define the *size* of f to be the maximum index i such that t_i appears among the variable symbols of f. Formally that is

$$\mathrm{size}(f) \;:=\; \max\{\, 1 \leq i \in \mathbb{N} \mid \exists\, \alpha : f[\alpha] \neq 0,\ \alpha_i \neq 0 \,\}$$

Note that this truly is finite, as there only are finitely many α such that $f[\alpha] \neq 0$ and for any $\alpha = (\alpha_i)$ there also are finitely many i only, such that $\alpha_i \neq 0$. As our exemplary ideal let us take the zero-ideal $\mathfrak{a} := 0$. By construction we have $(\bar{t}_i)^i = 0$ and hence $\bar{t}_i \in \sqrt{0}$. On the other hand we have (for any $n \in \mathbb{N}$ with $n < i$)

$$(\bar{t}_i)^n \;\in\; (\sqrt{0})^n \quad\text{but}\quad (\bar{t}_i)^n \neq 0$$

Thus for any $n \in \mathbb{N}$ let us just take some $i \in \mathbb{N}$ with $n < i$. Then $\bar{t}_i$ demonstrates that $(\sqrt{0})^n$ is not contained in 0. Also $\sqrt{0}$ is not finitely generated. Because if we consider a finite collection of elements

$\overline{f}_1,\ldots,\overline{f}_k \in \sqrt{0}$ then just take $i > \max\{\,\mathrm{size}(f_j) \mid j \in 1\ldots k\,\}$. Then it is clear that $f_j \in E[t_1,\ldots,t_{i-1}]$ and hence $t_i \notin \langle f_1,\ldots,f_k\rangle_{\mathfrak{i}}$. And thereby

$$\bar{t}_i \;\notin\; \langle f_1,\ldots,f_k\rangle_{\mathfrak{i}} \Big/ \mathfrak{v} \;=\; \langle \overline{f}_1,\ldots,\overline{f}_k\rangle_{\mathfrak{i}}$$

□

Proof of (2.31):

(i) Consider any $a \in R$, then $a \in \sqrt{\mathfrak{b}} \cap R$ is equivalent, to $\varphi(a) \in \sqrt{\mathfrak{b}}$. That is iff there is some $k \in \mathbb{N}$ such that $\varphi(a^k) = \varphi(a)^k \in \mathfrak{b}$. This again is $a^k \in \mathfrak{b} \cap R$, which is equivalent to $a \in \sqrt{\mathfrak{b} \cap R}$.

(ii) In order to prove $\sqrt{\mathfrak{a}}S \subseteq \sqrt{\mathfrak{a}S}$ we have to verify $\varphi(\sqrt{\mathfrak{a}}) \subseteq \sqrt{\mathfrak{a}S}$. Thus consider any $a \in \sqrt{\mathfrak{a}}$, that is $a^k \in \mathfrak{a}$ for some $k \in \mathbb{N}$. But from this we get $\varphi(a)^k = \varphi(a^k) \in \varphi(\mathfrak{a}) \subseteq \mathfrak{a}S$. And this again is $\varphi(a) \in \sqrt{\mathfrak{a}S}$, which had to be shown. Next, as $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$ we clearly have $\mathfrak{a}S \subseteq \sqrt{\mathfrak{a}}S$ which gives rise to the incusion

$$\sqrt{\mathfrak{a}S} \;\subseteq\; \sqrt{\sqrt{\mathfrak{a}}S}$$

Conversely consider any $f \in S$ such that $f^k \in \sqrt{\mathfrak{a}}\,S$ for some $k \in \mathbb{N}$. That is there are $g_i \in S$ and $a_i \in \sqrt{\mathfrak{a}}$ such that

$$f^k \;=\; g_1\varphi(a_1) + \cdots + g_n\varphi(a_n)$$

As a_i is contained in $\sqrt{\mathfrak{a}}$ there is some $k(i) \in \mathbb{N}$ such that $a_i^{k(i)} \in \mathfrak{a}$. Now let us abbreviate $b_i := \varphi(a_i)$, $l := k(1) + \cdots + k(n)$ and $m := k \cdot l$. Then we get

$$f^m \;=\; (g_1b_1 + \ldots g_nb_n)^l \;=\; \sum_{|\alpha|=l} \binom{l}{\alpha} (g_1b_1)^{\alpha(1)} \ldots (g_nb_n)^{\alpha(n)}$$

Now fix any α and suppose for any $i \in 1\ldots n$ we had $\alpha(i) < k(i)$, then we had $l = |\alpha| = \alpha(1) + \cdots + \alpha(n) < k(1) + \cdots + k(n) = l$ an obvious contradiction. Hence for any α there is some $j \in 1\ldots n$ such that $\alpha(j) \geq k(j)$. And for this j we get

$$b_j^{\alpha(j)} \;=\; b_j^{\alpha(j)-k(j)} b_j^{k(j)} \;=\; b_j^{\alpha(j)-k(j)} \varphi\left(a_j^{k(j)}\right) \;\in\; \mathfrak{a}\,S$$

But as this holds true for any α with $|\alpha| = l$ we find that $f^m \in \mathfrak{a}\,S$. And this again means that f is contained in the radical of $\mathfrak{a}\,S$.

(iii) The equivalence $\mathfrak{b}$ is a $\star$ iff $\varphi^{-1}(\mathfrak{b})$ is a $\star$ has already been proved in the correspondence theorem (1.66). Thus from now on φ is surjective, then $\varphi(\mathfrak{a})$ is a ideal of S due to (1.76). Now compute

$$\begin{aligned}
\varphi^{-1}\varphi(\mathfrak{a}) &= \{\, b \in R \mid \varphi(b) \in \varphi(\mathfrak{a}) \,\} \\
&= \{\, b \in R \mid \exists\, a \in \mathfrak{a} : \varphi(b) = \varphi(a) \,\} \\
&= \{\, b \in R \mid \exists\, a \in \mathfrak{a} : b - a \in \mathrm{kn}(\varphi) \,\} \\
&= \{\, b \in R \mid \exists\, a \in \mathfrak{a} : b \in a + \mathrm{kn}(\varphi) \,\} \\
&= \{\, a + \mathrm{kn}(\varphi) \mid a \in \mathfrak{a} \,\} \\
&= \mathfrak{a} + \mathrm{kn}(\varphi)
\end{aligned}$$

Now by the first claim $\mathfrak{b} := \varphi(\mathfrak{a})$ is a $\star$ iff $\varphi^{-1}(\mathfrak{b}) = \varphi^{-1}\varphi(\mathfrak{a}) = \mathfrak{a} + \mathrm{kn}(\varphi)$ is a $\star$. And this already is the second claim.

□

Proof of (2.33):

- The equivalence of (a) and (b): The implication (b) $\implies$ (a) is trivial: Let us abbreviate $\mathbb{V}^*(\mathfrak{a}) := \{\, \mathfrak{m} \in \mathrm{Smax}(R) \mid \mathfrak{a} \subseteq \mathfrak{m} \,\}$ then we can take this set to be $\mathcal{M}$. Thereby $\mathbb{V}^*(\mathfrak{a})$ is non-empty, as $\mathfrak{a}$ is proper and we have (2.4.(ii)). Now to (a) $\implies$ (b): Consider any $\mathfrak{m} \in \mathcal{M}$, as $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}} = \bigcap \mathcal{M} \subseteq \mathfrak{m}$ we find that $\mathcal{M} \subseteq \mathbb{V}^*(\mathfrak{a})$ and thereby

$$\bigcap \mathbb{V}^*(\mathfrak{a}) \quad \subseteq \quad \bigcap \mathcal{M} \quad = \quad \sqrt{\mathfrak{a}}$$

 Conversely, if $\mathfrak{m}$ is a maximal ideal containing $\mathfrak{a} \subseteq \mathfrak{m}$, then $\sqrt{\mathfrak{a}} \subseteq \sqrt{\mathfrak{m}} = \mathfrak{m}$, as any maximal ideal is prime and any prime ideal is radical. And as this is true for any $\mathfrak{m} \in \mathbb{V}^*(\mathfrak{a})$ we also find

$$\sqrt{\mathfrak{a}} \quad \subseteq \quad \bigcap \mathbb{V}^*(\mathfrak{a})$$

- The equivalence of (b) and (c): As any prime ideal is radical it satisfies $\sqrt{\mathfrak{p}} = \mathfrak{p}$ such that he implication (b) $\implies$ (c) is satisfied trivially. Conversely consider any proper ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$, for this - by (2.25.(i)) - we already know

$$\sqrt{\mathfrak{a}} \quad = \quad \bigcap \mathbb{V}(\mathfrak{a}) \quad = \quad \bigcap \{\, \mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{a} \subseteq \mathfrak{p} \,\}$$

 By assumption (c) any $\mathfrak{p}$ is the intersection of all maximal ideals of R containing $\mathfrak{p}$. Let us rewrite all this in a little more intuitive way

$$\sqrt{\mathfrak{a}} \quad = \quad \bigcap_{\mathfrak{a} \subseteq \mathfrak{p}} \mathfrak{p} \quad = \quad \bigcap_{\mathfrak{a} \subseteq \mathfrak{p}} \bigcap \{\, \mathfrak{m} \in \mathrm{Smax}(R) \mid \mathfrak{p} \subseteq \mathfrak{m} \,\} \quad = \quad \bigcap_{\mathfrak{a} \subseteq \mathfrak{p}\, \mathfrak{p} \subseteq \mathfrak{m}} \mathfrak{m}$$

 That is $\sqrt{\mathfrak{a}}$ is the intersection of all maximal ideals $\mathfrak{m}$ for which there is a prime ideal $\mathfrak{p}$ such that $\mathfrak{a} \subseteq \mathfrak{p}$ and $\mathfrak{p} \subseteq \mathfrak{m}$. We now claim that this amounts to

$$\sqrt{\mathfrak{a}} \quad = \quad \bigcap_{\mathfrak{a} \subseteq \mathfrak{p}\, \mathfrak{p} \subseteq \mathfrak{m}} \mathfrak{m} \quad = \quad \bigcap \{\, \mathfrak{m} \in \mathrm{Smax}(R) \mid \mathfrak{a} \subseteq \mathfrak{m} \,\}$$

 If there is some $\mathfrak{p} \in \mathrm{Spec}(R)$ such that $\mathfrak{a} \subseteq \mathfrak{p}$ and $\mathfrak{p} \subseteq \mathfrak{m}$, then $\mathfrak{a} \subseteq \mathfrak{m}$, as well. If conversely $\mathfrak{a} \subseteq \mathfrak{m}$, then we may just take $\mathfrak{p} := \mathfrak{m}$, as any maximal ideal also is prime. Thus the intersection runs over precisely the same set of maximal ideals $\mathfrak{m}$ and hence is equal.

- The equivalence of (c) and (e) is an immediate consequence of the correspondence theorem of ideals. Recall our abbreviation $\mathbb{V}^*(\mathfrak{p}) := \{\, \mathfrak{m} \in \mathrm{Smax}(R) \mid \mathfrak{p} \subseteq \mathfrak{m} \,\}$ then we evaluate the Jacobson-radical of $R/\mathfrak{a}$, using the correspondence (1.71)

$$\mathrm{JAC}\left(R/\mathfrak{p}\right) \quad = \quad \bigcap \mathrm{Smax}\left(R/\mathfrak{p}\right) \quad = \quad \bigcap \left\{ \mathfrak{m}/\mathfrak{p} \;\middle|\; \mathfrak{m} \in \mathbb{V}^*(\mathfrak{p}) \right\}$$

 The correspondence theorem (1.66.(ii)) also tells us that the intersection of ideals is compatible,

that is we can interchange intersection and quotient to arrive at

$$\textsc{jac}\left(R\big/\mathfrak{p}\right) \;=\; \bigcap \mathbb{V}^*(\mathfrak{p})\big/\mathfrak{p}$$

If (c) then $\bigcap \mathbb{V}^*(\mathfrak{p}) = \mathfrak{p}$ such that we find $\textsc{jac}(R/\mathfrak{p}) = \mathfrak{p}/\mathfrak{p} = 0$, which is (e). Conversely if (e), then by the correspondence of ideals we have $\bigcap \mathbb{V}^*(\mathfrak{p}) = \mathfrak{p}$, which is (c). Hence the equivalence.

- The equivalence of (b) and (d) is another consequence of the correspondence theorem of ideals. Let us evaluate also the nil-radical of $R/\mathfrak{a}$, using (1.71) again, we find

$$\textsc{nil}\left(R\big/\mathfrak{a}\right) \;=\; \bigcap \textsf{Spec}\left(R\big/\mathfrak{a}\right) \;=\; \bigcap \left\{ \mathfrak{p}\big/\mathfrak{a} \;\middle|\; \mathfrak{p} \in \mathbb{V}(\mathfrak{a}) \right\}$$

As before we can interchange intersection and quotient according to (1.66.(ii)), but this time we can also use (2.25.(i)), which is $\bigcap \mathbb{V}(\mathfrak{a}) = \sqrt{\mathfrak{a}}$, to arrive at

$$\textsc{nil}\left(R\big/\mathfrak{a}\right) \;=\; \bigcap \mathbb{V}(\mathfrak{a})\big/\mathfrak{a} \;=\; \sqrt{\mathfrak{a}}\big/\mathfrak{a}$$

We have already evaluated the Jacobson-radical of $R/\mathfrak{a}$ in the previous step (for this we did not use that $\mathfrak{p}$ was a prime ideal). So let us recollect the result

$$\textsc{jac}\left(R\big/\mathfrak{a}\right) \;=\; \bigcap \textsf{Smax}\left(R\big/\mathfrak{a}\right) \;=\; \bigcap \mathbb{V}^*(\mathfrak{a})\big/\mathfrak{a}$$

Now if (b), then we have $\sqrt{\mathfrak{a}} = \bigcap \mathbb{V}^*(\mathfrak{a})$ such that the nil- and Jacobson-radicals of $R/\mathfrak{a}$ coincide, which is (d). Conversely if (d), then by the correspondence of ideals we have $\sqrt{\mathfrak{a}} = \bigcap \mathbb{V}^*(\mathfrak{p})$, which is (b). Hence the equivalence.

- The equivalence of (e) and (f): Here (f) $\implies$ (e) is obvious: If $\mathfrak{p}$ is a prime ideal, then $S := R/\mathfrak{p}$ is an integral domain and $\varrho : R \to R/\mathfrak{p} : a \mapsto a + \mathfrak{p}$ is surjective. Hence we get $\textsc{jac}(R/\mathfrak{p}) = 0$ by (f). Conversely let $\mathfrak{p} := \textsf{kn}(\varphi)$, then by the first isomorphism theorem (1.83.(ii)) we obtain an isomorphism between $R/\mathfrak{p}$ and S by virtue of

$$\widetilde{\varphi} \;:\; R\big/\mathfrak{p} \;\xrightarrow{\sim}\; S \;:\; a + \mathfrak{p} \mapsto \varphi(a)$$

As S is an integral domain, so is $R/\mathfrak{p}$ and this means that $\mathfrak{p}$ is a prime ideal. Thus by (e) we have $\textsc{jac}(R/\mathfrak{p}) = 0$. But as $\widetilde{\varphi}$ is an isomorphism we thereby get

$$\begin{aligned} \textsc{jac}(S) \;&=\; \bigcap \{\, \mathfrak{n} \mid \mathfrak{n} \in \textsf{Smax}(S) \,\} \;=\; \bigcap \{\, \widetilde{\varphi}(\mathfrak{m}) \mid \mathfrak{m} \in \textsf{Smax}(R/\mathfrak{a}) \,\} \\ &=\; \widetilde{\varphi}\left(\bigcap \{\, \mathfrak{m} \mid \mathfrak{m} \in \textsf{Smax}(R/\mathfrak{a}) \,\} \right) \;=\; \widetilde{\varphi}\left(\textsc{jac}(R/\mathfrak{p})\right) \;=\; 0 \end{aligned}$$

□

Proof of (3.106):

- We will first prove the implication (a) $\implies$ (b): that is we regard a non-empty family $\mathcal{P} \subseteq \textsf{Subm}(M)$ of sumbodules of M. We will give a proof by contradiction, that is we suppose $\mathcal{P}$ had *no* maximal element. That is for any $P \in \mathcal{P}$ there is some $Q \in \mathcal{P}$ with $P \subseteq Q$ but $P \neq Q$. As $\mathcal{P}$ is non-empty we can start with some $P_0 \in \mathcal{P}$. Suppose we have already found $P_0 \subset P_1 \subset \ldots \subset P_k$ where

$P_i \in \mathcal{P}$. As $\mathcal{P}$ has no maximal elements P_k is not maximal, that is $P_k \subset P_{k+1}$ for some $P_{k+1} \in \mathcal{P}$. Continuing indefinitely we would find a non-stationary chain $P_0 \subset P_1 \subset \ldots \subset P_k \subset P_{k+1} \subset \ldots$ in contradiction to (a).

- Next let us prove (b) $\Longrightarrow$ (c): that is we are given any sub-module $Q \leq_{\mathsf{m}} M$ of M. To do this let us regard the set of finitly generated sub-modules of Q

$$\mathcal{P} \;:=\; \{\, P \leq_{\mathsf{m}} Q \mid P \text{ finitely generated} \,\}$$

Clearly $0 \in \mathcal{P}$, such that $\mathcal{P}$ is non-empty. By assumption (b) contains a maximal element $P^* \in \mathcal{P}$. Now for any $x \in Q$ it is clear that $P := P^* + \mathsf{Lh}(x)$ is another finitely generated sub-module of Q [clearly if $P^* = \mathsf{Lh}(x_1, \ldots, x_n)$ then $P = \mathsf{Lh}(x_1, \ldots, x_n, x)$]. That is $P \in \mathcal{P}$ again and $P^* \subseteq P$. By maximality of P^* this is $P^* = P$ and hence $x \in P = P^*$. As $x \in Q$ has been chosen arbitarily this means $Q \subseteq P^*$ and hence $Q = P^*$. In particular $Q \in \mathcal{P}$ is finitely generated itself.

- Let us first close the circle by proving (c) $\Longrightarrow$ (a): that is we regard some ascending chain $P_0 \subseteq P_1 \subseteq P_2 \subseteq \ldots$ of sub-modules $P_k \leq_{\mathsf{m}} M$ of M. As the P_k for a chain we know by (3.27.(v)) that the union

$$P \;:=\; \bigcup_{k \in \mathbb{N}} P_k \quad \leq_{\mathsf{m}} \quad M$$

is a sub-module of M again. And by assumption (c) it is finitely generated, that is $P = \mathsf{Lh}(x_1, \ldots, x_r)$ for some $x_i \in P$. That is for any $i \in 1 \ldots r$ there is some $k(i) \in \mathbb{N}$ such that $x_i \in P_{k(i)}$ now take $s := \max\{\, i(1), \ldots, i(r) \,\} \in \mathbb{N}$. Then - as the P_k for an ascending chain - we have $x_i \in P_{k(i)} \subseteq P_s$ again. In particular $P = \mathsf{Lh}(x_1, \ldots, x_r) \subseteq P_s$ such that for any $j \in \mathbb{N}$ we have $P \subseteq P_s \subseteq P_{s+j} \subseteq P$ which implies $P_{s+j} = P_s$. This means that the chain (P_k) becomes stationary at the index s, which proves (a).

□

Proof of (3.111):

(i) If M is $\star$ then P clearly is $\star$ as well, as any chain of sub-modules of P also is a chain of sub-modules of M. Also M/P is $\star$ again: by the corrspondence theorem (3.16.(ii)) any sub-module of M/P is of the form Q/P for some sub-module $Q \leq_{\mathsf{m}} M$. Hence any chain of sub-modules of M/P corresponds to a chain of sub-modules in M and hence stabilizes.

Conversely suppose both P and M/P are noetherian, then we have to prove that M is noetherian. To do this we regard an ascending chain of sub-modules

$$Q_0 \;\subseteq\; Q_1 \;\subseteq\; \ldots \subseteq\; Q_k \;\subseteq\; Q_{k+1} \;\subseteq\; \ldots$$

Then $Q_0 \cap P \subseteq Q_1 \cap P \subseteq Q_2 \cap P \subseteq \ldots$ is an ascending chain of sub-modules. As P is noetherian it stabilizes, that is there is some $r \in \mathbb{N}$ such that for any $i \in \mathbb{N}$ we have $Q_{r+i} \cap P = Q_r \cap P$. Also we obtain an ascending chain of sub-modules of M/P by

$$Q_0 + P \,\big/_P \;\subseteq\; Q_1 + P \,\big/_P \;\subseteq\; Q_2 + P \,\big/_P \;\subseteq\; \ldots$$

As M/P is noetherian as well this chain stabilizes, too, that is there is some $t \in \mathbb{N}$ such that for all $i \in \mathbb{N}$ we have $(Q_{t+i} + P)/P = (Q_t + P)/P$. By the correspondense theorem this already is $Q_{t+i} + P = Q_t + P$. Now choose $s := \max(r, t)$, then for any $i \in \mathbb{N}$ we have

$$Q_{s+i} \cap P \;=\; Q_s \cap P \quad \text{and} \quad Q_{s+i} + P \;=\; Q_s + P$$

Now by the modular rule (3.17) this implies $Q_{s+i} = Q_s$ which means that M is noetherian, as well.

In case that both P and M/P are artinian, we regard a descending chain $Q_0 \supseteq Q_1 \supseteq Q_2 \supseteq \ldots$ and use the same arguments as above to show that it stabilizes, as well. All we have to do is replace any "$\subseteq$" by "$\supseteq$".

(iv) Clearly M is isomorphic to the sub-module $M \oplus 0$ of $M \oplus N$ by virtue of $M \xrightarrow{\sim} M \oplus 0 : x \mapsto (x, 0)$. Also it is clear that N is isomorphic to the quotient $(M \oplus N)/(M \oplus 0)$ under the isomorhism

$$N \;\xrightarrow{\sim}\; M \oplus N \Big/ {}_{M \oplus 0} \;:\; y \mapsto (0, y) + (M \oplus 0)$$

Thus regarding $M \oplus 0$ as a sub-module of $M \oplus N$ we know that $M \oplus N$ is $\star$ if and only if both $M \oplus 0$ and $(M \oplus N)/(M \oplus 0)$ are $\star$. But due to the isomorphisms this again is equivalent to both M and N being $\star$.

(ii) It is really easy to see, that $M/(P \cap Q)$ can be embedded into $(M/P) \oplus (M/Q)$ by virtue of the following map

$$M \Big/ {}_{P \cap Q} \hookrightarrow M \Big/ {}_{P} \oplus M \Big/ {}_{Q} \;:\; x + (P \cap Q) \mapsto (x + P, x + Q)$$

Because, if $x + P = y + P$ and $x + Q = y + Q$ then we have both $x - y \in P$ and $x - y \in Q$. And this means $x - y \in P \cap Q$ which yields $x + (P \cap Q) = y + (P \cap Q)$. Hence the above map is injective. As both M/P and M/Q are $\star$ so is $(M/P) \oplus (M/Q)$ according to (iv). But as $M/(P \cap Q)$ is isomorphic to a sub-module of $(M/P) \oplus (M/Q)$ and this isomorphic copy is $\star$ according to (i), so is $M/(P \cap Q)$.

(v) As $\varphi : M \twoheadrightarrow N$ is surjective, the first isomorphism theorem (3.78.(ii)) yields an isomorphism $M/\mathrm{kn}(\varphi) \xrightarrow{\sim} N$ by virtue of $x + \mathrm{kn}(\varphi) \mapsto \varphi(x)$. In particular N is isomprphic to a quotient module $M/\mathrm{kn}(\varphi)$ of M. Now, as M is $\star$, we find that $M/\mathrm{kn}(\varphi)$ is $\star$ due to (i) and hence N is $\star$ because of the isomorphy.

(iii) As P and Q are $\star$ by (iv) we know that $P \oplus Q$ is $\star$. But clearly there is a surjective R-module homomorphism $P \oplus Q \twoheadrightarrow P + Q$ by letting $(x, y) \mapsto x + y$. The surjectivity is trivial and the R-linearity is obvious: $a(x, y) = (ax, ay) \mapsto ax + ay = a(x + y)$ and $(u, v) + (x, y) = (u + x, v + y) \mapsto (u + x) + (v + y) = (u + v) + (x + y)$. Hence by (v) we find that $P + Q$ is $\star$ again, as it is an epimorphic image of $P \oplus Q$.

(vi) Since M is finitely generated we can choose some generators $x_k \in M$, that is $M = \mathrm{Lh}(x_1, \ldots, x_n)$. Then we clearly have an R-module epimorphism by letting

$$R^n \twoheadrightarrow M \;:\; (a_1, \ldots, a_n) \mapsto \sum_{i=k}^{n} a_k x_k$$

As R is $\star$ as a ring it also is $\star$ as an R-module (in fact this even is equivalent). Using (iv) and induction on n it is clear that $R^n = R \oplus R \oplus \cdots \oplus R$ (n-times) is $\star$ again. Hence M is $\star$, by (v), as it is an epimorphic image of a $\star$ module.

(vii) Let us denote the R-module homomorphisms by $\varphi : L \hookrightarrow M$ and $\psi : M \twoheadrightarrow N$, that is we regard the following exact chain

$$0 \to L \xrightarrow{\varphi} M \xrightarrow{\psi} N \to 0$$

As ψ is injective we find that $\mathrm{kn}(\psi) = \mathrm{im}(\varphi)$ is isomorphic to L under $L \to \mathrm{kn}(\psi) : x \mapsto \varphi(x)$. And as ψ is surjective, by the first isomorphism theorem (3.78.(ii)), we also get the isomorphism

$$M \Big/ \mathrm{kn}(\psi) \xrightarrow{\sim} N \ : \ y + \mathrm{kn}(\psi) \mapsto \psi(y)$$

By (i) we know, that M is $\star$ if and only if both $\mathrm{kn}(\psi)$ and $M/\mathrm{kn}(\psi)$ are $\star$. And due to the above isomorphisms, this now is equivalent to both L and N being $\star$.

□

Proof of (3.110):

- Suppose $P \subseteq \mathbb{Q}$ is a finitely generated $\mathbb{Z}$-sub-module of $\mathbb{Q}$. That is there are some $x_k = a_k/b_k$ (where $k \in 1 \dots n$) that generate P, then we let $b := b_1 b_2 \dots b_n$ and $\widehat{b_k} := b/b_k \in \mathbb{Z}$. Then any element of P is of the form

$$\sum_{k=1}^{n} r_k \frac{a_k}{b_k} \ = \ \sum_{k=1}^{n} \frac{r_k a_k \widehat{b_k}}{b} \ = \ \left(\sum_{k=1}^{n} r_k a_k \widehat{b_k} \right) \frac{1}{b} \ \in M_b$$

- Suppose $M \subseteq \mathbb{Q}$ was maximal and choose any $q \in \mathbb{Q}$ with $q \notin M$. Then $M + \mathbb{Z}q = \mathbb{Q}$, as M was maximal. Hence we find an epimorphism

$$\mathbb{Z} \twoheadrightarrow \mathbb{Q} \Big/ M \ : \ k \mapsto kq + M$$

Let $n\mathbb{Z}$ be the kernel of this homomorphism, then we have an isomorphy of $\mathbb{Z}_n \xrightarrow{\sim} \mathbb{Q}/M$ under the correspondence $k + n\mathbb{Z} \mapsto kq + M$. Composing the canonical epimorphism $\mathbb{Q} \twoheadrightarrow \mathbb{Q}/M : x \mapsto x + M$ with the inverse $\mathbb{Q}/M \xrightarrow{\sim} \mathbb{Z}_n$ we find another epimorphism

$$\varphi \ : \ \mathbb{Q} \twoheadrightarrow \mathbb{Z}_n \ : \ x \mapsto x + M = kq + M \mapsto k + n\mathbb{Z}$$

But a homomorphism of this form always is zero: Let $e := \varphi(1/1)$, then for any prime p we have $e = \varphi(p/p) = p\varphi(1/p)$. That is $p \mid e$ for any prime p and this only leaves $e = 0$. From this reasoning we then get $0 = e = \varphi(b/b) = b\varphi(1/b)$ for any $b \neq 0$, which means $\varphi(1/b) = 0$, such that $\varphi = 0$ altogether.

In particular $\varphi(q) = 0 + n\mathbb{Z}$, but $q + M$ also corresponds to $1 + n\mathbb{Z}$ such that $0 + n\mathbb{Z} = 1 + n\mathbb{Z}$, which means $n = 1$. That is $q + M = 0 + M$ or in other words $q \in M$. This finally is a contradiction, that can only be remedied, by dropping the assumption of the maximality of M.

□

Proof of (3.113):
The implication (b) $\implies$ (c) is easy to see, since any noetherian module V already is finitely generated. Conversely for (c) $\implies$ (b) we note that any field is noetherian - as it contains two ideals only. And as $V \cong_{\mathfrak{m}} F^n$ by assumption, it is the (n-times) direct product of a noetherian module and hence noetherian itself, according to (3.111.(iv))
The same argument holds true for (c) $\implies$ (a): Since F also is artinian and $V \cong_{\mathfrak{m}} F^n$ just is a finite direct sum of this, we likewise find that V is artinian, too. So it only remains to prove (a) $\implies$ (c): To do this let us start with a basis $\{ v_i \mid i \in I \}$ of V. To begin with, we let $I_0 := I$. Suppose I_0 to I_k have already been constructed, then we commence: If $I_k \neq \emptyset$ still is non-empty, choose some arbitrary $i(k+1) \in I_k$ and let $I_{k+1} := I_k \setminus \{ i(k+1) \}$. Always take $U_k := \mathrm{Lh}\{ v_i \mid i \in I_k \}$ the subspace generated by the v_i where $i \in I_k$. This means $U_k = U_{k+1} + Fv_{i(k+1)}$ and in particular $U_{k+1} \subset U_k$ [if we had $v_{i(k+1)} \in U_{k+1}$ this would contradict the linear independence of the basis]. Thus we found a strictly descending chain of subspaces

$$V = U_0 \supset U_1 \supset \ldots \supset U_n \supset \ldots$$

But since V is artinian, this chain has to stabilize, that is there is some $n \in \mathbb{N}$ such that we cannot continue our construction. And this can only occur if $I_n = \emptyset$, which means, that I was finite. □

Proof of (3.114):

- (a) $\implies$ (b): given any $x \in M$ with $x \neq 0$ we clearly know, that $P = Rx \leq_{\mathfrak{m}} M$ is a sub-module of M. And since $x = 1\,x \in P$ we have $P \neq 0$, which only leaves $M = Rx$, by assumption (a).

- (b) $\implies$ (a): consider any sub-module $P \leq_{\mathfrak{m}} M$ of M. If $P = 0$, then there is nothing to prove, else pick up some $x \in P$ with $x \neq 0$. Now we get $M = Rx$ by assumption (b), but as also $M = Rx \subseteq P \subseteq M$ this implies $P = M$.

- (b) $\implies$ (c): choose any $x \in M$ with $x \neq 0$, which is possible since $M \neq 0$ is non-zero. By assumption (b) we then have $M = Rx$. Now let $\mathfrak{m} := \mathrm{ann}(x) \trianglelefteq_{\mathfrak{i}} R$. Then by (3.22.(ii)) we have the following isomorphy of R-modules

 $$\Phi : R\big/_{\mathrm{ann}(x)} \xrightarrow{\sim} M : b + \mathrm{ann}(x) \mapsto bx$$

 Now suppose $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$ is an ideal of R such that $\mathfrak{m} \subseteq \mathfrak{a}$. Then the above isomorphy transfers $\mathfrak{a}/\mathfrak{m}$ to a sub-module $P = \Phi(\mathfrak{a}) \leq_{\mathfrak{m}} M$ of M. But as (b) implies (a) this means $P = 0$ or $P = M$. In case $P = 0$ we have $\mathfrak{a} = \mathfrak{m}$ and in case $P = M$ we have $\mathfrak{a} = R$. This shows that $\mathfrak{m}$ even is a maximal ideal of M.

- (c) $\implies$ (a): suppose $\Phi : R/\mathfrak{m} \xrightarrow{\sim} M$ is that isomorphism of R-modules and consider some sub-module $P \leq_{\mathfrak{m}} M$ of M. Then $\mathfrak{a} := \Phi^{-1}(P) \leq_{\mathfrak{m}} R/\mathfrak{m}$ is an R-sub-module of $R/\mathfrak{m}$. As R is commutative it is clear that $\mathfrak{a}$ even is an ideal of $R/\mathfrak{m}$. But as $\mathfrak{m}$ is maximal, the only ideals of $R/\mathfrak{m}$ are 0 and $R/\mathfrak{m}$ itself. In case $\mathfrak{a} = 0$ we see $P = \Phi(\mathfrak{a}) = 0$ and in case $\mathfrak{a} = R/\mathfrak{m}$ we find $P = \mathrm{im}(\Phi) = M$. Hence 0 and M are the only sub-modules of M, as has been claimed in (a).

□

Proof of (3.117):
For the moment being - as long as we have not proved that the length of M is uniquely determined - let us denote by $\ell(M)$ the *minimum* length of of a composition series of M

$$\ell(M) \;:=\; \min\{\, r \in \mathbb{N} \mid (M_0, M_1, \ldots, M_r) \text{ composition series of } M \,\}$$

Also, given any two sub-modules U and $V \leq_{\mathsf{m}} M$, we denote the set of all chains of sub-modules that start in P and end in Q by $\mathcal{C}(U,V)$, that is

$$\mathcal{C}(U,V) \;:=\; \left\{ (P_0, P_1, \ldots, P_r) \;\middle|\; \begin{array}{l} \forall\, i \in 0 \ldots r : P_i \leq_{\mathsf{m}} M \\ U = P_0 \subset P_1 \subset \ldots \subset P_r = V \end{array} \right\}$$

And we say that two chains $(P_0, P_1, \ldots, P_r)$ and $(Q_0, Q_1, \ldots, Q_s)$ in $\mathcal{C}(U,V)$ are *equivalent*, written as $(P_{0,1}, \ldots, P_r) \sim (Q_0, Q_1, \ldots, Q_s)$, iff $r = s$ and there is some permutation $\sigma \in S_r$ such that for any $i \in 1 \ldots r$ we have the following isomorphy of the quotient modules

$$P_i \Big/ P_{i-1} \;\cong_{\mathsf{m}}\; Q_{\sigma(i)} \Big/ Q_{\sigma(i)-1}$$

And in this case we say that σ *assigns* the equivalence of $(P_0, P_1, \ldots, P_r)$ and $(Q_0, Q_1, \ldots, Q_r)$. Thereby $\sim$ truly is an equivalence relation: clearly $(P_0, P_1, \ldots, P_r) \sim (P_0, P_1, \ldots, P_r)$ is assigned by the identity $\mathbb{1} \in S_r$. And if $(P_0, P_1, \ldots, P_r) \sim (Q_0, Q_1, \ldots, Q_s)$ is assigned by $\sigma \in S_r$ then the reverse relation $(Q_0, Q_1, \ldots, Q_s) \sim (P_0, P_1, \ldots, P_r)$ is assigned by the inverse permutation $\sigma^{-1} \in S_r$. And finally, if $(N_0, N_1, \ldots, N_r) \sim (P_0, P_1, \ldots, P_s)$ is assigned by σ and $(P_0, P_1, \ldots, P_s) \sim (Q_0, Q_1, \ldots, Q_t)$ is assigned by τ then we also get the equivalence $(N_0, N_1, \ldots, N_r) \sim (Q_0, Q_1, \ldots, Q_t)$ that is assigned by the composition $\tau\sigma$, since

$$N_i \Big/ N_{i-1} \;\cong_{\mathsf{m}}\; P_{\sigma(i)} \Big/ P_{\sigma(i)-1} \;\cong_{\mathsf{m}}\; Q_{\tau(\sigma(i))} \Big/ Q_{\tau(\sigma(i))-1}$$

(i) Let $(M_0, M_1, \ldots, M_r)$ be a composition series of M of minimal length $r = \ell(M)$ and denote $P_i := M_i \cap P$. Let us also denote

$$\varphi_i \;:\; P_i \to M_i \Big/ M_{i-1} \;:\; x \mapsto x + M_{i-1}$$

then it is clear that $\mathrm{kn}(\varphi_i) = M_{i-1} \cap P = P_{i-i}$. Hence we find an R-module-monorphism (this is the first isomorphism theorem)

$$\Phi_i \;:\; P_i \Big/ P_{i-1} \;\hookrightarrow\; M_i \Big/ M_{i-1} \;:\; x + P_{i-1} \mapsto x + M_{i-1}$$

That is P_i/P_{i-1} is isomorphic to a sub-module of M_i/M_{i-1}. But as M_i/M_{i-1} is a simple module this implies $P_i/P_{i-1} = 0$ (which yields $P_i = P_{i-1}$) or Φ_i even is an isomorphism (which yields that P_i/P_{i-1} is simple again). Altogether

$$P_i \;=\; P_{i-1} \quad \text{or} \quad \Phi_i \text{ is an isomorphism}$$

Let us now omit those P_i with $P_i = P_{i-1}$, that is if we take to the index set $I := \{\, i \in 1 \ldots r \mid P_i \neq P_{i-1} \,\}$ and $q := (\#I) - 1$ then we may renumber the index set $I = \{\, \alpha(0), \alpha(1), \ldots, \alpha(q) \,\}$ with $0 = \alpha(0) <$

$\alpha(1) < \cdots < \alpha(q)$ and thereby obtain a composition series of P

$$0 \;=\; P_{\alpha(0)} \;\subset\; P_{\alpha(1)} \;\subset\; \ldots \;\subset\; P_{\alpha(q)} \;=\; P$$

Thereby $P_{\alpha(q)} = M_r \cap P = M \cap P = P$. Hence we have obtained a composition series of P of length $q \leq r$. Suppose we had $q = r$, then we did not omit any $i \in 0 \ldots r$, that is Φ_i is an isomorphsim for any $i \in 1 \ldots r$. Then we can prove $P_i = M_i$ for any $i \in 0 \ldots r$ by induction on r: Clearly $P_0 = 0 = M_0$ and if $P_{i-1} = M_{i-1}$ then, as Φ_i is surjective, it is just the identity map on M_i/M_{i-1}. In particular we get $P = M \cap P = M_r \cap P = P_r = M_r = M$ which contradicts the assumption $P \neq M$.

(iii) Recall that a composition series $(M_0, M_1, \ldots, M_r)$ of M is an element of $\mathcal{C}(0, M)$ such that every quotient M_i/M_{i-1} is simple. We will now prove, that any two composition series $(M_0, M_1, \ldots, M_r)$ and $(N_0, N_1, \ldots, N_s)$ of M are equivalent. Without loss of generality let us assume $r \leq s$, then we will use induction on the length r of the shorter chain. To be precise the induction hypothesis will be: If $(M_0, M_1, \ldots, M_r)$ and $(N_0, N_1, \ldots, N_s)$ are two composition series of some module $M_r = N_s$ of length $r \leq s$, then $(M_0, M_1, \ldots, M_r) \sim (N_0, N_1, \ldots, N_s)$ are equivalent already.

For $r = 0$ we have $0 = M_0 = M_r = M$, that is $M = 0$ and hence $s = 0$, too. Thus for $r = 0$ there is nothing to prove. Also if $r = 1$ then $M = M/0 = M_1/M_0$ and hence M is simple. Therefore $(0, M)$ is the only composition series of M, as M admits no other sub-modules. So from now on we only have to regard $r \geq 2$ and can assume that the induction hypothesis is already proved for length $\leq r - 1$.

As a first case let us assume $M_{r-1} \subseteq N_{s-1}$. Then we find the inclusions $M_{r-1} \subseteq N_{s-1} \subseteq M = M_r$. But as M_r/M_{r-1} is simple this already means $M_{r-1} = N_{s-1}$ as $N_{s-1} \neq N_s = M = M_r$. Hence

$$(M_0, M_1, \ldots, M_{r-1}) \;\sim\; (N_0, N_1, \ldots, N_{s-1})$$

by induction hypothesis. But as $M_r/M_{r-1} = M/M_{r-1} = M/N_{s-1} = N_s/N_{s-1}$ even is an equality of R-modules it is clear that this equivalence extends to an equivalence of the same chains, appended by M

$$(M_0, M_1, \ldots, M_{r-1}, M_r) \;\sim\; (N_0, N_1, \ldots, N_{s-1}, N_s)$$

Likewise, as a second case, we suppose $N_{s-1} \subseteq M_{r-1}$ then the inclusions $N_{s-1} \subseteq M_{r-1} \subseteq M = N_s$ imply $M_{r-1} = N_{s-1}$ as N_s/N_{s-1} is simple and $M_{r-1} \neq M_r = M = N_s$. Thus this case ends up in the same equivalence, as the first case.

So in the last case we may assume $M_{r-1} \not\subseteq N_{s-1}$ and $N_{s-1} \not\subseteq M_{r-1}$. Then we find the inclusions $M_{r-1} \subset M_{s-1} + N_{s-1} \subseteq M = M_r$ such that we get the equality $M_{r-1} + N_{s-1} = M$. Now let $P := N_{s-1} \neq M$ and $P_i := M_i \cap P$ as in (i) above. As we have seen there is some $q < r$ such that $\alpha(0) < \alpha(1) < \cdots < \alpha(q)$ satisfies

$$\{\, \alpha(0), \alpha(1), \ldots, \alpha(q) \,\} \;=\; I \;=\; \{\, i \in 1 \ldots r \mid P_i \neq P_{i-1} \,\}$$

Suppose we had $P_{r-1} = P_r = M_r \cap P = P$, then $M_{r-1} \cap P = P_{r-1} = P$ implies $N_{s-1} = P \subseteq M_{r-1}$

which has already been dealt with. Hence we have $P_r \neq P_{r-1}$ that is $r \in I$ and hence necessarily $\alpha(q) = r$. Let us finally abbreviate $Q_i := P_{\alpha(i)} = M_{\alpha(i)} \cap P$, then $Q_q = P_{\alpha(q)} = P_r = M_r \cap P = P = N_{s-1}$. Also, as $P_{r-1} \neq P_r$ we find from the construction of the $\alpha(i)$ that $Q_{q-1} = P_{r-1}$ (even though it might well be, that $P_{r-2} = P_{r-1}$ but this does not bother us). As we have seen in (i) the Q_i then form a composition series of $P = N_{s-1}$

$$0 \;=\; Q_0 \;\subset\; Q_1 \;\subset\; \ldots \;\subset\; Q_q \;=\; N_{s-1}$$

That is $(Q_0, Q_1, \ldots, Q_{q-1}, Q_q) = (Q_0, Q_1, \ldots, Q_{q-1}, N_{s-1})$. And as as $q \leq r-1$ we may use the induction hypothesis to obtain the equivalence $(Q_0, Q_1, \ldots, Q_{q-1}, N_{s-1}) \sim (N_0, N_1, \ldots, N_{s-1})$. In particular we may append these chains by N_s to finally arrive at

$$(Q_0, Q_1, \ldots, Q_{q-1}, N_{s-1}, N_s) \;\sim\; (N_0, N_1, \ldots, N_{s-1}, N_s)$$

We will now prove the equivalence of $(Q_0, Q_1, \ldots, Q_{q-1}, M_{r-1}, M_r)$ and $(Q_0, Q_1, \ldots, Q_{q-1}, N_{s-1}, N_s)$ which will be assigned by the transposition $\tau = (q-1\,q)$. That is we will prove the following isomorphies

$$M_{r-1}\Big/_{Q_{q-1}} \;\xrightarrow{\sim}\; N_s\Big/_{N_{s-1}} \;:\; x + Q_{q-1} \mapsto x + N_{s-1}$$

$$N_{s-1}\Big/_{Q_{q-1}} \;\xrightarrow{\sim}\; M_r\Big/_{M_{r-1}} \;:\; x + Q_{q-1} \mapsto x + M_{r-1}$$

The injectivity is clear from the definition, if $x \in M_{r-1}$ with $x + N_{s-1} = 0 + N_{s-1}$ then $x \in M_{r-1} \cap N_{s-1} = Q_{q-1}$. And likewise, if $x \in N_{s-1}$ with $x + M_{r-1} = 0 + M_{r-1}$ then $x \in N_{s-1} \cap M_{r-1} = Q_{q-1}$ again. Hence M_{r-1}/Q_{q-1} is isomorphic to a sub-module of the simple module N_s/N_{s-1}. But $M_{r-1} = Q_{q-1} = M_{r-1} \cap P$ would mean $M_{r-1} \subseteq P = N_{s-1}$ which has been dealt with in the first case. Hence here $x + Q_{q-1} \mapsto x + N_{s-1}$ is an isomorphism. Likewise N_{s-1}/Q_{q-1} is isomorphic to a sub-module of the simple module M_r/M_{r-1} but $N_{s-1} = Q_{q-1} = M_{r-1} \cap N_{s-1}$ would imply $N_{s-1} \subseteq N_{s-1}$ which has been dealt with in the second case. Hence $x + Q_{q-1} \mapsto x + M_{r-1}$ is an isomorphism, as well.

But as $q \leq r-1$ we may use the induction hypothesis once more to get the equivalence $(Q_0, Q_1, \ldots, Q_{q-1}, M_{r-1}) \sim (M_0, M_1, \ldots, M_{r-2}, M_{r-1})$. And again this can be appended, to $(Q_0, Q_1, \ldots, Q_{q-1}, M_{r-1}, M_r) \sim (M_0, M_1, \ldots, M_{r-2}, M_{r-1}, M_r)$. So summarizing all the results we have finally proved, that

$$\begin{aligned}(N_0, N_1, \ldots, N_{s-2}, N_{s-1}, N_s) \;&\sim\; (Q_0, Q_1, \ldots, Q_{q-1}, N_{s-1}, N_s)\\ &\sim\; (Q_0, Q_1, \ldots, Q_{q-1}, M_{r-1}, M_r)\\ &\sim\; (M_0, M_1, \ldots, M_{r-2}, M_{r-1}, M_r)\end{aligned}$$

(ii) Let $(P_0, P_1, \ldots, P_k)$ be a composition series of P and $(Q_0, Q_1, \ldots, Q_n)$ be a composition series of M/P. Due to the correspondence theorem any sub-module Q_i of M/P is of the form $Q_i = M_i/P$ for some sub-module $M_i \leq_{\mathfrak{m}} M$ with $P_k = P \subseteq M$. Then we get

$$M_1\Big/_{P_k} \;=\; M_1\Big/_{P} \;=\; Q_1 \;\cong_{\mathfrak{m}}\; Q_1\Big/_{0} \;=\; {}^{P_1}\Big/_{P_0}$$

That is: as P_1/P_0 is simple, so is M_1/P_k. Also due to the third isomorphism theorem (3.78) we

also find for any $i \in 1 \dots n$

$$Q_i \Big/ Q_{i-1} \;=\; M_i/P \Big/ M_{i-1}/P \;\xrightarrow{\sim}\; M_i \Big/ M_{i-1}$$

where this isomorphism is given by $(x+P)+(M_{i-1}/P) \mapsto x + M_{i-1}$ which is not important however. Thereby we have found, that any M_i/M_{i-1} is simple again, such that we can assemble a composition series of M by letting $(P_0, P_1, \dots, P_k, M_1, \dots, M_n)$. In particular M is of finite length and we have found the equality

$$\ell(M) \;=\; k+n \;=\; \ell(P) + \ell\left(M \Big/ P\right)$$

It remains to prove that conversely, if M has finite length, then P and M/P have finite length, too. The case of P has already been shown in (i), it remains to prove this for M/P. Hence let $(M_0, M_1, \dots, M_r)$ be a composition series of M, then we define

$$Q_i \;:=\; M_i + P \Big/ P \;\leq_{\mathsf{m}}\; M \Big/ P$$

It is clear that $Q_0 = P/P = 0$ and $Q_r = (M+P)/P = M/P$. And the third isomorphism theorem (3.78) yields the following isomorphy

$$M_i + P \Big/ M_{i-1} + P \;\cong_{\mathsf{m}}\; (M_i+P)/P \Big/ (M_{i-1}+P)/P \;=\; Q_i \Big/ Q_{i-1}$$

Explicitly this isomorphism is $x + (M_{i-1}+P) \mapsto (x+P) + Q_{i-1}$ but this doesn't matter, really. Let us now regard the following map

$$\Phi_i \;:\; M_i \Big/ M_{i-1} \;\to\; M_i + P \Big/ M_{i-1} + P \;:\; x + M_{i-1} \mapsto x + (M_{i-1} + P)$$

It is clear that Φ_i is surjective, given any $x \in M_i$ and $p \in P$ we see that $x + M_{i-1} \mapsto x + (M_{i-1} + P) = x + p + (M_{i-1} + P)$. And the kernel of Φ_i is obviously given to be

$$\mathsf{kn}(\Phi_i) \;=\; M_i \cap (M_{i-1}+P) \Big/ M_{i-1} \;\leq_{\mathsf{m}}\; M_i \Big/ M_{i-1}$$

But as M_i/M_{i-1} is simple this either means $\mathsf{kn}(\Phi_i) = 0$ (and hence Φ_i is injective, thereby bijective) or $\mathsf{kn}(\Phi_i) = M_i/M_{i-1}$ (and thereby $M_i \cap (M_{i-1}+P) = M_i$ which means $M_i \subseteq M_{i-1}+P$ such that $M_i + P = M_{i-1} + P$ which implies $Q_i = Q_{i-1}$). Altogether we have

$$M_i + P = M_{i-1} + P \;\text{ or }\; \Phi_i \text{ is an isomorphism}$$

Let us now take $I := \{\, 1 \dots r \mid Q_i \neq Q_{i-1} \,\}$, then for any $i \in I$ we have that Φ_i is an isomorphism, such that

$$M_i \Big/ M_{i-1} \;\cong_{\mathsf{m}}\; M_i + P \Big/ M_{i-1} + P \;\cong_{\mathsf{m}}\; Q_i \Big/ Q_{i-1}$$

That is for any $i \in I$ we find that Q_i/Q_{i-1} is a simple module. And for any $j \notin I$ we have seen $Q_j = Q_{j-1}$. Therefore we can pick up some indexes $0 \leq \alpha(0) < \alpha(1) < \dots < \alpha(n) \leq r$ such that $I = \{\, \alpha(0), \alpha(1), \dots, \alpha(n) \,\}$ and have found a composition series of M/P by $(Q_{\alpha(0)}, Q_{\alpha(1)}, \dots, Q_{\alpha(n)})$. In particular M/P has finite length again and the equivalence holds true.

We now turn our attention to the generalization of the above statement for any ascending chain $0 = P_0 \subseteq P_1 \subseteq P_2 \subseteq \ldots \subseteq P_n = M$ of sub-modules of M. For $n = 1$ the equality is clear, as $P_1/P_0 = M/0 = M$. For general n we use induction on n. By the above, we have

$$\ell(M) \;=\; \ell\left(M \Big/ P_{n-1}\right) + \ell\big(P_{n-1}\big)$$

Note that $P_n = M$ and use the induction hypothesis on P_{n-1} then we may express the length of P_{n-1} [and thereby of M] as the sum

$$\ell(M) \;=\; \ell\left(P_n \Big/ P_{n-1}\right) + \sum_{k=1}^{n-1} \ell\left(P_k \Big/ P_{k-1}\right) \;=\; \sum_{k=1}^{n} \ell\left(P_k \Big/ P_{k-1}\right)$$

(v) Without loss of generality we may assume $P_0 = 0$ and $P_k = M$. Because if $P_0 \neq 0$ or $P_k \neq M$ then we may append the series $(P_0, \ldots, P_k)$ to $(0, P_0, P_1, \ldots, P_k, M)$ which we will refine instead.

We will now prove this statement by induction on the length $r = \ell(M)$ of M. If $r = 0$ we have $M = 0$ and hence the only series of sumbodules of M is (0) which is a composition series already. Likewise for $r = 1$ we know that M is simple, such that $(0, M)$ is the only series of sub-modules which is a composition series already. Thus let us now assume the refinement-property has been established for any series of sub-modules in any R-module of length $r - 1$ or less.

If $k \leq 1$ then any composition series of M appends $(P_0, P_1) = (0, M)$. And as M was assumed to have finite length, there is some composition series. Thus we may regard the case $k \geq 2$. Then $0 \subset P_1 \subset M$ such that by (i) we have $\ell(P_1) < \ell(M) = r$ and by (ii) also $\ell(M/P_1) = \ell(M) - \ell(P_1) < \ell(M) = r$. By induction hypothesis we hence get a refinement $(L_0, L_1, \ldots, L_p)$ of $(0, P_1)$, that is $L_0 = 0$ and $L_p = P_1$. And denoting $Q_i := P_i/P_1$ for $i \in 1 \ldots k$, the induction hypothesis also yields a refinement $(N_1, N_2, \ldots, N_q)$ of $(Q_1, \ldots, Q_k)$. Thereby N_i is of the form $N_i = M_i/P_1$ for some $M_i \leq_{\mathsf{m}} M$ due to the correspondence theorem of modules. Therefore

$$M_{\alpha(i)} \Big/ P_1 \;=\; N_{\alpha(i)} \;=\; Q_i \;=\; P_i \Big/ P_1$$

which yields $M_{\alpha(i)} = P_i$ for $i \in 1 \ldots k$. We have seen in (ii) that $(L_0, L_1, \ldots, L_p, M_2, \ldots, M_q)$ is a composition series of M. And any P_i can be found inside of this composition series: $P_0 = L_0$, $P_1 = L_p = M_1$ and $P_i = M_{\alpha(i)}$ for any $i \in 2 \ldots k$. Hence $(L_0, L_1, \ldots, L_p, M_2, \ldots, M_q)$ is the refinement of $(P_0, P_1, \ldots, P_k)$ we sought.

(iv) It is clear that $\leq$ is a partial order on $\mathcal{C}(0, M)$, so we only have to prove the three equivalences. (a) $\implies$ (b): consider any refinement $(M_0, M_1, \ldots, M_r) \leq (N_0, N_1, \ldots, N_s)$, then by (v) we can choose a refinement of $(N_0, N_1, \ldots, N_s)$ to a composition series $(C_0, C_1, \ldots, C_t)$ of M. By (ii) the composition series has length $t = \ell(M) = r$. And thereby $r \leq s \leq t = r$ implies $r = s$, which means $(M_0, M_1, \ldots, M_r) = (N_0, N_1, \ldots, N_s)$. (b) $\implies$ (c): now suppose $(M_0, M_1, \ldots, M_r)$ was no composition series of M, that is there is some $i \in 1 \ldots r$ and some $Q \leq_{\mathsf{m}} M$ such that $M_{i-1} \subset Q \subset M_i$. Then we already had a true refinement of $(M_0, M_1, \ldots, M_r)$ by

$$(M_0, \ldots, M_r) \;<\; (M_0, \ldots, M_{i-1}, Q, M_i, \ldots, M_r)$$

such that $(M_0, M_1, \ldots, M_r)$ could not have been maximal. Finally the implication (c) $\implies$ (a) has

already been proved in (iii).

(vi) Consider any $\varphi_i : M_{i-1} \to M_i$ then, by the first isomorphism theorem, we have $M_{i-1}/\mathrm{kn}(\varphi_i) \xrightarrow{\sim} \mathrm{im}(\varphi_i)$ and hence by (ii)

$$\ell(\mathrm{kn}(\varphi_i)) + \ell(\mathrm{im}(\varphi_i)) \;=\; \ell(\mathrm{kn}(\varphi_i)) + \ell\left(M_{i-1} \Big/ \mathrm{kn}(\varphi_i)\right) \;=\; \ell(M_{i-1})$$

Now recall that the i-th homology module is defined by $H_i := \mathrm{kn}(\varphi_{i+1})/\mathrm{kn}(\varphi_i)$, then the claim follows by easy computation using (ii) again

$$\begin{aligned}
\sum_{i=0}^{n}(-1)^i\ell(H_i) &= \sum_{i=0}^{n}(-1)^i\ell\left(\mathrm{kn}(\varphi_{i+1}) \Big/ \mathrm{kn}(\varphi_i)\right) \\
&= \sum_{i=0}^{n}(-1)^i\left[\ell(\mathrm{kn}(\varphi_{i+1})) - \ell(\mathrm{kn}(\varphi_i))\right] \\
&= \sum_{i=1}^{n+1}(-1)^{i-1}\ell(\mathrm{kn}(\varphi_{i+1})) - \sum_{i=0}^{n}(-1)^i\ell(\mathrm{kn}(\varphi_i)) \\
&= \sum_{i=1}^{n}(-1)^{i-1}\left[\ell(\mathrm{kn}(\varphi_i)) + \ell(\mathrm{kn}(\varphi_i))\right] \\
&\quad +(-1)^n\ell(\mathrm{kn}(\varphi_{n+1})) - \ell(\mathrm{im}(\varphi_0)) \\
&= \sum_{i=1}^{n}(-1)^{i-1}\ell(M_i) + (-1)^n\ell(M_n) - \ell(0) \\
&= \sum_{i=0}^{n}(-1)^i\ell(M_i)
\end{aligned}$$

□

Proof of (3.119):
Let us denote the quotient ring $Q := R/\mathrm{ann}(M)$. If now M is an R-module, then M can also be turned into a Q-module under the scalar multiplication $(b + \mathrm{ann}(x)) := bx$ as has been shown in (3.22.(v)). And from this construction it is clear that (for any $X \subset M$)

$$\mathrm{Lh}_R(X) \;=\; \mathrm{Lh}_Q(X)$$

In particular the Q-sub-modules of M are precisely the R-sub-modules of M. And therefore it is equivalent whether M is noetherian (resp. artinian) as an R-module or an an Q-module. This will be used in the proof of (i) and (ii).

(i) If M is noetherian, then in particular it is finitly generated by property (c) of noetherian modules. And also, if M is noetherian, then M^n is noetherian by (3.111.(iv)). But by (3.23.(iv)) we find an embedding $Q \hookrightarrow M^n$ of R-modules (where $n = \mathrm{rank}(M)$). That is, there is an isomorphic copy of Q as an R-sub-module of M^n. As M^n is noetherian this implies, that Q is a noetherian R-module, hence a noetherian Q-module and hence a noetherian ring.

Conversely suppose Q is a noetherian ring and M a finitly generated R-module. Then Q is finitely generated as an Q-module (using the same generators) and hence a noetherian Q-module by virtue of (3.111.(vi)). But this again means that M is a noetherian R-module, as well.

(ii) If M is artinian, then M^n is artinian by (3.111.(iv)). But by (3.23.(iv)) we find an embedding $Q \hookrightarrow M^n$ of R-modules (where $n = \mathrm{rank}(M)$, which is finite by assumption). That is, there is an isomorphic copy of Q as an R-sub-module of M^n. As M^n is artinian this implies, that Q is an artinian R-module, hence an artinian Q-module and hence an artinian ring.

Conversely suppose Q is an artinian ring and M a finitely generated R-module. Then Q is finitely generated as an Q-module (using the same generators) and hence an artinian Q-module by virtue of (3.111.(vi)). But this again means that M is an artinian R-module, as well.

(iii) If M is finitely generated and artinian then $Q = R/\mathrm{ann}(M)$ is an artinian ring by virtue of (ii). But from (2.40.(ii)) we know that any artinian ring already is noetherian. Hence Q is noetherian and M is finitely generated, such that M is noetherian by (i).

(iv) Let us regard $K_n := \mathrm{kn}(\varphi^n) \leq_{\mathfrak{m}} M$, then it is clear that the K_n form an ascending chain of sub-modules of M

$$K_0 \subseteq K_1 \subseteq K_2 \subseteq \dots$$

As M is noetherian this chain has to stabilize at some point $s \in \mathbb{N}$, that is $K_{s+1} = K_s$. Now consider any $y \in \mathrm{kn}(\varphi)$, as φ is surjective so is $\varphi^s : M \to M$. Hence there is some $x \in M$ such that $y = \varphi^s(x)$. Now $0 = \varphi(y) = \varphi(\varphi^s(x)) = \varphi^{s+1}(x)$ that is $x \in K_{s+1} = K_s$. That is $y = \varphi^s(x) = 0$ which implies that φ already is injective, as well.

(v) Let us regard $I_n := \mathrm{im}(\varphi^n) \leq_{\mathfrak{m}} M$, then it is clear that the I_n form a descending chain of sub-modules of M

$$I_0 \supseteq I_1 \supseteq I_2 \supseteq \dots$$

As M is artinian this chain has to stabilize at some point $s \in \mathbb{N}$, that is $I_{s+1} = I_s$. Now consider any $y \in M$, as $\pi^s(y) \in I_s = I_{s+1}$ there is some $x \in M$ such that $\varphi^s(y) = \varphi^{s+1}(x) = \varphi^s(\varphi(x))$. As φ is injective, so is $\pi^s : M \to M$ and hence we find $y = \varphi(x)$. As y has been arbitrariy this means that φ already is surjective.

(vi) Let us first suppose that $r = \ell(M) < \infty$ that is M admits a composition series $(M_0, M_1, \dots, M_r)$. We will prove that M is noetherian and artinian by induction on r. If $r = 0$ then $M = 0$ so there is nothing to prove. And if $r = 1$ then M is simple and hence $0 \subseteq M$ is the only chain of sub-modules of M. In particular M is noetherian and artinian. Let now r be aritrary and suppose the claim has been proved for any module of length less than r. As M_1 is simple it is noetherian and artinian as we have argued for $r = 1$. Also by (3.117.(ii)) we have $\ell(M/M_1) = \ell(M) - \ell(M_1) < \ell(M) = r$ so by induction hypothesis M/M_1 is noetherian and arininan too. But (3.111.(i)) now implies that M is noetherian and artinian, as well.

Conversely suppose M is both, artinian and noetherian. Then we have to prove that M is of finite length. To do this define the set $\mathcal{K}$ of all those sub-modules of M that have a composition series

$$\mathcal{K} := \{ K \leq_{\mathfrak{m}} M \mid \ell(K) < \infty \}$$

As $0 \in \mathcal{K}$ we see that $\mathcal{K}$ is non-empty and hence (as M is noetherian) has a maximal element $K^* \in \mathcal{K}$. By construction K^* has a composition series, say $(K_0, K_1, \dots, K_r)$. Now suppose we had

$K^* \neq M$, then we take to the set $\mathcal{L}$ of all sub-modules of M that strictly contain K^*

$$\mathcal{L} \;:=\; \{\, L \;\leq_{\mathsf{m}}\; M \mid K^* \subset L \,\}$$

As $K^* \neq M$ we have $M \in \mathcal{L}$ such that $\mathcal{L}$ is non-empty. Hence (as M also is artinian) there is a minimal element $L_* \in \mathcal{L}$. Now suppose there is some sub-module $P \leq_{\mathsf{m}} M$ with $K^* \subseteq P \subseteq L_*$. If $P \neq K^*$ then $P = L_*$ as L_* is minimal with this property. That is L_*/K^* is simple and hence we find a composition series of L_* by $(K_0, K_1, \ldots, K_r, L_*)$. But remember, K^* has been maximal among those sub-modules of M that admit a composition series so it cannot be extended to $K^* \subset L_*$. Hence the assumption $K^* \neq M$ has to be false and in particular $M = K^*$ itself has a composition series.

(vii) We start with (d) $\implies$ (b), but in fact we have just seen in (vi) that a module of finite length is both, artinian and noetherian. For (b) $\implies$ (c) there is nothing to do either, as *any* sub-module of a noetherian module is finitely generated - in particular M itself. And (c) $\implies$ (a) is true, since R was assumed to be artinian and we have (3.111.(vi)). So it only remains to prove (a) $\implies$ (d): Let $\mathfrak{j} := \textsc{jac}(R)$ be the Jacobson radical of R. As R is artinian $\mathfrak{j}$ is nilpotent, that is there is some $n \in \mathbb{N}$ such that $\mathfrak{j}^n = 0$, due to (2.40.(v)). Now define (for any $k \in 1 \ldots n$)

$$Q_k \;:=\; \mathfrak{j}^{k-1}M \Big/ \mathfrak{j}^k M$$

e.g. $Q_1 = M/\mathfrak{j}M$. As $\mathfrak{j}^{k-1}M$ is a sub-module of M it is artinian, too and hence Q_k is artinian, being the quotient of an artinian module. We will now prove, that any Q_k has finite length only. This will then ensure, that M is of finite length, as well, since by the remark (iii) following the theorem of Jordan-Hölder (3.117) we know

$$\ell(M) \;=\; \sum_{k=1}^{n} \ell(Q_k)$$

Let $S := R/\mathfrak{j}$, then Q_k can be regarded as an S-module, as any sub-module of Q_k allows the scalar multiplication $(a + \mathfrak{j})(x + \mathfrak{j}^k M) = ax + \mathfrak{j}^k M$. ?? Grünes Buch S. 563 Aufgabe 2

(viii) First of all (e) $\implies$ (d), as for any $i \in 1 \ldots n$ we can take $N_i := M_1 \oplus \cdots \oplus M_i \oplus 0 \oplus \cdots \oplus 0 \;\leq_{\mathsf{m}} M$. To be precise also let $N_0 := 0 \;\leq_{\mathsf{m}} M$ then for any $i \in 1 \ldots n$ we clearly have the isomprphy $M_i \;\xrightarrow{\sim}\; N_i/N_{i-1} : x_i \mapsto x_i + M_{i-1}$ and in particular M_i/M_{i-1} is simple, by assumption (e). Therefore $(N_0, N_1, \ldots, N_r)$ is a composition series of M such that $\ell(M) = r < \infty$ is finite.

The implications (d) $\implies$ (a) and (d) $\implies$ (b) have already been shown in (vi). Also (b) $\implies$ (c) is clear, as *any* sub-module of a noetherian module is finitely generated, in particular M itself.

We will now prove (c) $\implies$ (e): as M is finitely generated we may pick up some $x_k \in M$ such that $M = \mathrm{Lh}(x_1, \ldots, x_n)$. By assumption M is semi-simple, that is there are some simple sub-modules $M_i \leq_{\mathsf{m}} M$ such that

$$M \;=\; \bigoplus_{i \in I} M_i$$

That is any x_k can be written as a *finite* sum of some elements $x_{k,i} \in M_i$ and hence there is some

finite subset $\Omega(k) \subseteq I$ such that

$$x_k \;=\; \sum_{i\in\Omega(k)} x_{k,i}$$

As $n \in \mathbb{N}$ is finite and any $\Omega(k) \subseteq I$ is finite, so is the union $\Omega := \Omega(1) \cup \cdots \cup \Omega(n)$ of these sets. And as the x_k generate M we see that M in fact is a finite direct sum, as claimed

$$M \;=\; \bigoplus_{i\in\Omega} M_i$$

Hence we have established the chain (e) $\implies$ (d) $\implies$ (b) $\implies$ (c) $\implies$ (e). And as we already know (d) $\implies$ (a) as well, it suffices to prove (a) $\implies$ (e): as M is semi-simple we have $M = \oplus_i M_i$ as above. Thereby we may omit all those $i \in I$ with $M_i = 0$. Now suppose I was infinite, then there was some injection $\alpha : \mathbb{N} \hookrightarrow I$. Then we take $I(k) := I \setminus \{\, \alpha(j) \mid j \leq k \,\}$ for any $k \in \mathbb{N}$ and let

$$N_k \;:=\; \bigoplus_{i\in I(k)} M_i$$

Then it is clear that the N_k form a strictly descending chain of sub-modules of M, that is $N_0 \supset N_1 \supset N_2 \supset \ldots$ in contradiction to M being artinian. Hence I could not have been infinite such that (e) holds true.

If now M even is a vector-space, that is R is a field, then clearly M is finitely generated if and only if M is finite dimensional. Hence (f) is equivalent to (c) and therefore to any other of the statements, as well.

(ix) Let us denote the set of all ideal-induced sub-modules $\mathfrak{a}M$ of M such that $M/\mathfrak{a}M$ *is* noetherian by $\mathcal{P}$

$$\mathcal{P} \;:=\; \left\{\, \mathfrak{a}M \mid \mathfrak{a} \trianglelefteq_{\mathrm{i}} R,\; {}^{M}\big/_{\mathfrak{a}M} \text{ is not noetherian} \,\right\}$$

Suppose M was not noetherian, then $0 \in \mathcal{P}$ and hence $\mathcal{P}$ is not empty. By assumption and (0.25) $\mathcal{P}$ then contains a maximal element $\mathfrak{a}^*M$. Let us now denote

$$M' \;:=\; {}^{M}\big/_{\mathfrak{a}^*M} \quad\text{and}\quad A \;:=\; {}^{R}\big/_{\mathrm{ann}(M')}$$

Then A is a commutative ring again and we can regard M' as an A-module. Note that by construction M' is *not* noetherian. Now, given any ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} A$ in A, by the correspondence theorem $\mathfrak{a}$ is of the form $\mathfrak{a} = \mathfrak{b}/\mathrm{ann}(M')$ for some $\mathfrak{b} \trianglelefteq_{\mathrm{i}} R$ with $\mathrm{ann}(M') \subseteq \mathfrak{b}$. We will now prove

$$\mathfrak{a}^* \;\subseteq\; \mathfrak{b}$$

To do this regard any $a \in \mathfrak{a}^*$ then for any $x \in M$ we get $ax \in \mathfrak{a}^*M$. That is $a(x + \mathfrak{a}^*M) = ax + \mathfrak{a}^*M = 0 + \mathfrak{a}^*M$ and hence $a \in \mathrm{ann}(M') \subseteq \mathfrak{b}$. As a has been arbitrary this proves $\mathfrak{a}^* \subseteq \mathrm{ann}(M') \subseteq \mathfrak{b}$. Now, by construction it is clear that $\mathfrak{a}M' = \mathfrak{b}M/\mathfrak{a}^*M$. And thereby the third isomorphism theorem yields

$${M'}\big/_{\mathfrak{a}M'} \;=\; {M/\mathfrak{a}^*M}\big/_{\mathfrak{b}M/\mathfrak{a}^*M} \;\cong_{\mathrm{m}}\; {M}\big/_{\mathfrak{b}M}$$

But as $\mathfrak{a}^* \subseteq \mathfrak{b}$ and $\mathfrak{a}^*$ has been maximal this implies either $\mathfrak{a}^* = \mathfrak{b}$ (and hence $\mathfrak{a} = 0$) or $M'/\mathfrak{a}M'$

is noetherian. Now let

$$\mathcal{Q} \;:=\; \left\{ Q \leq_{\mathfrak{m}} M' \mid \operatorname{ann}_A\left(M' \Big/ Q\right) = 0 \right\}$$

Recall $A = R/\operatorname{ann}_R(M')$ and that the scalar multiplication of M' (with A) is defined by $(a + \operatorname{ann}(M'))(x + \mathfrak{a}^* M) = ax + \mathfrak{a}^* M$. Therefore we have $\operatorname{ann}_A(M') = \operatorname{ann}_R(M')/\operatorname{ann}_R(M') = 0 \subseteq A$ such that $0 \in \mathcal{Q}$. In particular $\mathcal{Q}$ is non-empty.

If now $(Q_i) \subseteq \mathcal{Q}$ is a chain in $\mathcal{Q}$ then we take $Q := \bigcup_i Q_i$ to be the union of the Q_i. As (Q_i) is a chain Q is a sub-module of M' again. Consider any $a \in A$ with $a \in \operatorname{ann}_A(M'/Q) = 0$, that is $a(M'/Q) = 0$ or in other words $aM' \subseteq Q$. As M is finitely generated, so is M' say $M' = \mathrm{Lh}(x_1, \ldots, x_n)$, then we have $ax_k \in Q$ for any $k \in 1 \ldots n$ and hence $ax_k \in Q_{i(k)}$ for some $i(k) \in I$. As the Q_i form a chain we may take Q_i to be the maximum of $Q_{i(1)}$ to $Q_{i(n)}$. Then for any $k \in 1 \ldots n$ we have $ax_k \in Q_i$. But as the x_k generate M' this implies $aM' \subseteq Q_i$ and therefore $a \in \operatorname{ann}(M'/Q_i) = 0$ such that $a = 0$. That is $\operatorname{ann}_A(M'/Q) = 0$ and hence $Q \in \mathcal{Q}$ again. Hence any chain (Q_i) of $\mathcal{Q}$ has an upper bound Q and hence the lemma of Zorn yields a maximal element Q^* of $\mathcal{Q}$. Now take to

$$M'' \;:=\; M' \Big/ Q^*$$

If $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} A$ is any ideal with $\mathfrak{a} \neq 0$ then by (3.40.(v)) we have $\mathfrak{a}M'' = (\mathfrak{a}M' + Q^*)/Q^*$. Therefore the third isomorphism theorem again yields

$$M'' \Big/ \mathfrak{a}M'' \;=\; M'/Q^* \Big/ (\mathfrak{a}M' + Q^*)/Q^* \;\cong_{\mathfrak{m}}\; M' \Big/ \mathfrak{a}M' + Q^*$$

As we have shown before we have $\mathfrak{a}^* \subseteq \mathfrak{b}$ for $\mathfrak{a} = \mathfrak{b}/\operatorname{ann}(M')$. But as $\mathfrak{a} \neq 0$ and $\mathfrak{a}^*$ has been maximal we find that $M'/\mathfrak{a}M'$ is noetherian. But as we also have an epimorphism

$$M' \Big/ \mathfrak{a}M' \;\twoheadrightarrow\; M' \Big/ \mathfrak{a}M' + Q^*$$

This implies that $M'/(\mathfrak{a}M' + Q^*)$ is noetherian. By the above isomorphism, this makes $M''/\mathfrak{a}M''$ noetherian. So at last we have arrived at an A-module $N := M''$ that satisfies the following two properites

$$\forall\, \mathfrak{a} \trianglelefteq_{\mathfrak{i}} A \,:\, \mathfrak{a} \neq 0 \implies N \Big/ \mathfrak{a}N \text{ is noetherian}$$

$$\forall\, Q \leq_{\mathfrak{m}} N \,:\, Q \neq 0 \implies \operatorname{ann}\left(N \Big/ Q\right) \neq 0$$

We will now prove that $N = M''$ is noetherian by showing, that any sub-module of N is finitely generated: So suppose $Q \leq_{\mathfrak{m}} N$ is any sub-module of N. If $Q = 0$ then there is nothing to show, else there is some $a \in A$ with $a \neq 0$ such that $a(N/Q) = 0$, that is $aN \subseteq Q$. But as $aA \neq 0$ we know that N/aN is noetherian and hence $Q/aN \leq_{\mathfrak{m}} N/aN$ is finitely generated. And as M is finitely generated, so are $N = M''$ and aN. But as both Q/aN and aN are finitely generated (3.96) tells us that Q is finitely generated.

By now we have established that $N = M'' = M\ /Q^*$ is noetherian. Therefore (i) implies that $A/\operatorname{ann}(N)$ is a noetherian ring. Yet by construction we have $\operatorname{ann}(N) = \operatorname{ann}(M'/Q^*) = 0$ such that $A/\operatorname{ann}(N) = A$. That is A is a noetherian ring. Yet M' is a finitely generated A-module such that (3.111.(vi)) implies that $M' = M/\mathfrak{a}^* M$ *is* noetherian. But we have constructed M' is such a

way, as to be *not* noetherian. This contradiction can only be solved, if M has been noetherian from the start.

□

Proof of (2.46):

(i) If R is a field, then it clearly is an integral domain and artinin, as well as in this case the only ideals of R are 0 and R itself. In the converse direction regard any $0 \neq a \in R$, then we obtain a descending chain of ideals

$$aR \supseteq a^2R \supseteq \ldots \supseteq a^nR \supseteq a^{n+1}R \supseteq \ldots$$

Since R is artinian this chain has to stabilize, say at $n \in \mathbb{N}$. Hence $a^n \in a^nR = a^{n+1}R$. That is there is some $b \in R$ such that $a^n = a^{n+1}b$ which yields $a^n(1-ab) = 0$. But since R also is an integral domain and $a \neq 0$ this implies $ab = 1$ and hence $a \in R^*$ is invertible. Since $a \neq 0$ has been arbitrary this means, that R is a field.

(iii) If $\mathfrak{p} \trianglelefteq_{\mathfrak{i}} R$ is a prime ideal, then $Q := R/\mathfrak{p}$ is an integral domain by (2.12) and artinian by (2.40.(i)). But in (i) we have seen, that hence Q must be a field and hence $\mathfrak{p}$ is a maximal ideal, according to (2.5). This means we have proved

$$\mathrm{Spec}(R) = \mathrm{Smax}(R)$$

Now consider any prime ideal $\mathfrak{p} \trianglelefteq_{\mathfrak{i}} R$, by (2.18.(iv)) there is a minimal prime ideal $\mathfrak{p}_*$ underneath $\mathfrak{p}$ - that is $\mathfrak{p}_* \subseteq \mathfrak{p}$, just take $\mathfrak{a} = 0$ to impose no restrictions. But since $\mathfrak{p}_*$ is prime, it already is maximal in the artinian ring R. Hence we get $\mathfrak{p}_{ast} = \mathfrak{p}$. And as $\mathfrak{p}$ has been arbitrary, this shows >that any prime ideal of R already is minimal

$$\mathrm{Spec}(R) = \mathrm{Smin}(R)$$

(iv) Suppose $\{ \mathfrak{m}_i \mid i \in \mathbb{N} \}$ were infinitely many distinct maximal ideals of R. Then by (2.9) we would get a strictly descending chain of ideals in R, by taking to

$$\mathfrak{m}_1 \supset \mathfrak{m}_1\mathfrak{m}_2 \supset \mathfrak{m}_1\mathfrak{m}_2 \ldots \mathfrak{m}_n \supset \mathfrak{m}_1\mathfrak{m}_2 \ldots \mathfrak{m}_n\mathfrak{m}_{n+1} \supset \ldots$$

But this of course contradicts R being an artinian ring. Hence R could only have had finitely many maximal ideals, to begin with.

(v) Let $\mathfrak{j} := \mathrm{JAC}(R)$ be the jacobson radical of R, then we regard the following descending chain of ideals of R

$$\mathfrak{j} \supseteq \mathfrak{j}^2 \supseteq \ldots \supseteq \mathfrak{j}^n \supseteq \mathfrak{j}^{n+1} \supseteq \ldots$$

Since R is artinian this chain has to stabilize, that is there is some $n \in \mathbb{N}$ such that $\mathfrak{j}^n = \mathfrak{j}^{n+1}$. Suppose we had $\mathfrak{j}^n \neq 0$, then set of ideals $\mathcal{A} := \{ \mathfrak{a} \trianglelefteq_{\mathfrak{i}} R \mid \mathfrak{j}^n\mathfrak{a} \neq 0 \} \neq \emptyset$ would be non-empty, as it contains R. Still R is artinian so we may choose a minimal ideal $\mathfrak{a} \in \mathcal{A}_*$ satisfying $\mathfrak{j}^n\mathfrak{a} \neq 0$. Now we observe

$$\mathfrak{j}^n(\mathfrak{j}\mathfrak{a}) = \mathfrak{j}^{n+1}\mathfrak{a} = \mathfrak{j}^n\mathfrak{a} \neq 0$$

That is $\mathfrak{ja}$ is another ideal satisfying $\mathfrak{j}^n(\mathfrak{ja}) \neq 0$. But as $\mathfrak{a}$ was minimal with this property and also $\mathfrak{ja} \subseteq \mathfrak{a}$ we must have $\mathfrak{ja} = \mathfrak{a}$.

On the other hand, since $\mathfrak{ja} \neq 0$ there have to be some $j \in \mathfrak{j}$ and $a \in \mathfrak{a}$ such that $ja \neq 0$. Therefore $\mathfrak{j}(aR) \neq 0$, as well. And as $\mathfrak{a}$ has been minimal with this property and $aR \subseteq \mathfrak{a}$ we also find that $\mathfrak{a} = aR$ is a principal ideal. In particular $\mathfrak{a}$ is a finitely generated R-module.

Now, as $\mathfrak{j}^n \subseteq \mathfrak{j} = \text{JAC}(R)$ and $\mathfrak{j}^n\mathfrak{a} = \mathfrak{a}$ we may apply Nakayama's lemma (3.44.(ii)) to find $\mathfrak{a} = 0$. This of course contradicts $\mathfrak{j}^n\mathfrak{a} \neq 0$. So $\mathfrak{a}$ could not have been chosen in the first place, which means $\mathcal{A} = \emptyset$. But this can only happen, if $\mathfrak{j}^n = 0$ already.

Finally consider any $j \in \mathfrak{j} = \text{JAC}(R)$, then j already has to be nilpotent, as $j^n \in \mathfrak{j}^n = 0$. As this is true for any $j \in \mathfrak{j}$ we have shown the first inclusion in the chain [refer to (2.25.(ii))]

$$\text{JAC}(R) \subseteq \text{NIL}(R) = \bigcap \text{Spec}(R) \subseteq \text{Smax}(R) = \text{JAC}(R)$$

(vi) By (iv) we already know that R has finitely many maximal ideals only, say $\{ \mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_r \}$ And in (v) we have seen that the nil radical is the jacobson radical

$$\text{NIL}(R) = \text{JAC}(R) = \bigcap_{i=1}^{r} \mathfrak{m}_i$$

But as (powers of) distinct maximal ideals are coprime $\mathfrak{m}_i + \mathfrak{m}_j = R$ according to (2.9) we may just employ the Chinese remainder theorem (1.99.(iii)) to find precisely the isomorphism of the claim.

(vii) Again let $\{ \mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_r \}$ be the set of distinct maximal ideals of R. Also let $\mathfrak{j} = \text{JAC}(R)$ be the jacobson radical of R, of which we know $\mathfrak{j}^n = 0$ due to (v). Then we compute

$$\bigcap_{i=1}^{r} \mathfrak{m}_i^n \subseteq \left(\bigcap_{i=1}^{r} \mathfrak{m}_i \right)^n = \mathfrak{j}^n = 0$$

Note that the ideals $\mathfrak{a}_i := \mathfrak{m}_i^n$ are coprime, since they are powers of maximal ideals (2.9) such that the Chinese remainder theorem (1.99.(iii)) once again yields our isomorphy

$$R \Big/ \mathfrak{a} \cong_{\text{r}} \bigoplus_{i=1}^{r} R \Big/ \mathfrak{a}_i$$

As we have argued above we find $\mathfrak{a} = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_r = 0$, such that $R/\mathfrak{a}$ is canonically isomorphic to R. Also any of the rings $L_i := R/\mathfrak{a}_i$ is a local ring, as it is one of the examples following proposition (2.136). Its maximal ideal is given to be $\mathfrak{m}_i/\mathfrak{a}_i$.

(ii) Let us first assume, R is a local, artinian ring and denote its maximal ideal by $\mathfrak{m}$. Then clearly $\mathfrak{m} = \text{JAC}(R)$ and hence there is some $n \in \mathbb{N}$ such that $\mathfrak{m}^n = 0$, according to (v). Now regard

$$Q_k := \mathfrak{m}^{k-1} \Big/ \mathfrak{m}^k$$

e.g. $F := Q_1 = R/\mathfrak{m}$ is a field. The other Q_k are R-modules, but we can also consider them to be F-vector spaces under the scalar multiplication $(a + \mathfrak{m})(x + \mathfrak{m}^k) = ax + \mathfrak{m}^k$. Since R is artinian (as an R-module) so are its sub-modules $\mathfrak{m}^{k-1}$. Hence the Q_k are artinian R-modules,

being quotients of such. As any R-sub-module of Q_k already is a F-subspace, the R-sub-modules and F-subspaces are precisely the same sets (3.40.(ix)). Hence they also are artinian as F-vector spaces.

But by (3.113) this means that any Q_k is finite-dimensional vector space and hence noetherian. As both $Q_n \cong_{\mathfrak{m}} \mathfrak{m}^{n-1}$ and $Q_{n-1} = \mathfrak{m}^{n-2}/\mathfrak{m}^{n-1}$ are noetherian, so is $\mathfrak{m}^{n-2}$, according to (3.111.(i)). By induction we find that R is noetherian as an R-module and hence as a ring.

If R is not local, then by (vii) it still is isomorphic to a direct sum of local artinian rings L_i. And as we have just seen, any L_i is a noetherian ring. Hence by (2.40.(iii)) $L_1 \oplus \cdots \oplus L_r$ is a noetherian ring, due to the isomorphy, so is R.

□

Proof of (2.37):
Let $\mathcal{I} := \{ \mathfrak{a} \subseteq R \mid \mathfrak{a} \trianglelefteq_{\mathfrak{i}} R \}$ denote the set of ideals of R. Then we can install a partial order on $\mathcal{I}$ by letting $\mathfrak{a} \leq \mathfrak{b}$ if and only is $\mathfrak{b} \subseteq \mathfrak{a}$. Then the equivalence (a) $\iff$ (b) is just an application of (0.25) to the partially ordered set $(\mathcal{I}, \leq)$.

The main part (a) $\implies$ (f) of the theorem has already been proved in (ii), (iv) and (v) of (2.46). And the implication (f) $\implies$ (e) is easy to see: We need to prove $\mathrm{Spec}(R) \subseteq \mathrm{Smax}(R)$, so let $\mathfrak{p} \trianglelefteq_{\mathfrak{i}} R$ be any prime ideal of R. By assumption $\sqrt{0} = \mathrm{NIL}(R) = \mathrm{JAC}(R) = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r$ where $\mathfrak{m}_1$ to $\mathfrak{m}_r$ are the distinct maximal ideals of R. Then by (2.9)

$$\mathfrak{m}_1 \cdot \ldots \cdot \mathfrak{m}_r \;=\; \mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_r \;=\; \sqrt{0} \;\subseteq\; \mathfrak{p}$$

and as $\mathfrak{p}$ is prime, this means $\mathfrak{m}_i \subseteq \mathfrak{p}$ for some $i \in 1 \ldots r$. But as $\mathfrak{m}_i$ is maximal and $\mathfrak{p} \neq R$ this implies $\mathfrak{m}_i = \mathfrak{p}$ and in particular $\mathfrak{p}$ is maximal.

The next step (e) $\implies$ (d) uses another major theorem, the structure theorem of noetherian modules (5.14). By assumption R is a noetherian ring and thereby a noetherian R module. Hence there is a finite ascending chain of sub-modules

$$0 \;=\; M_0 \;\subset\; M_1 \;\subset\; \ldots \;\subset\; M_n \;=\; R$$

where every quotient $Q_k := M_k/M_{k-1}$ is isomorphic (as an R-module) to $R/\mathfrak{p}_k \xrightarrow{\sim} Q_k$ for some prime ideal $\mathfrak{p}_k \in \mathrm{Spec}(R)$. But by assumption we have $\mathrm{Spec}(R) = \mathrm{Smax}(R)$ these $\mathfrak{p}_k \trianglelefteq_{\mathfrak{i}} R$ already are maximal and hence $\ell(R/\mathfrak{p}_k) = 1$, as $0 \subset R/\mathfrak{p}_k$ is the one and only composition series of $R/\mathfrak{p}_k$. In particular we find

$$\ell(R) \;=\; \sum_{k=1}^{n} \ell(Q_k) \;=\; \sum_{k=1}^{n} 1 \;=\; n \;<\; \infty$$

The last step (d) $\implies$ (a) is trivial, as any (descending or ascending) chain of ideals (equivalently of R-sub-modules) has $\ell(R)$ as an upper bound.

By now, we have established the equivalences of (a), (b) and of (a), (d), (e), (f). Let us now prove the equivalences of (a), (c): If $\neg$ (a) then there is a strictly decreasing chain of ideals $\mathfrak{a}_0 \supset \mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \ldots$ such that $\mathcal{A} := \{ \mathfrak{a}_0, \mathfrak{a}_1, \mathfrak{a}_2, \ldots \}$ is totally ordered under $\subseteq$, but infinite. That is we then also get $\neg$ (b).

Conversely suppose ¬ (c), that is there is an infinite set $\mathcal{A}$, that is totally ordered under $\subseteq$. We start by choosing any $\mathfrak{a}_0 \in \mathcal{A}$. Suppose we had already chosen $\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \ldots \subset \mathfrak{a}_n$ from $\mathcal{A}$, then we continue: First we choose any other $\mathfrak{a} \in \mathcal{A} \setminus \{ \mathfrak{a}_0, \mathfrak{a}_1, \ldots, \mathfrak{a}_n \}$, then we distinguish 3 cases: (1) If $\mathfrak{a}_n \subseteq \mathfrak{a}$ then we may simply take $\mathfrak{a}_{n+1} := \mathfrak{a}$ and have appended our chain, to $\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \ldots \subset \mathfrak{a}_n \subset \mathfrak{a}_{n+1}$. (2) If $\mathfrak{a} \subseteq \mathfrak{a}_0$ then we have $\mathfrak{a} \subset \mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \ldots \subset \mathfrak{a}_n$. Thus all we have to to is shift the numbering of the $\mathfrak{a}_i$ to $\mathfrak{a}_{i+1}$ and call $\mathfrak{a}_0 := \mathfrak{a}$. (3) If neither (1) or (2), then let

$$k \;:=\; \max\{\, i \in 1 \ldots n \mid a_{i-1} \subseteq \mathfrak{a} \,\}$$

Then we get $\mathfrak{a}_0 \subset \ldots \subset \mathfrak{a}_{k-1} \subset \mathfrak{a} \subset \ldots \subset \mathfrak{a}_n$. Thus by renumbering these ideals (from k on) we are able to append our chain of ideals to $\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \ldots \subset \mathfrak{a}_n \subset \mathfrak{a}_{n+1}$ again. As we can do this indefinitely we conclude that $\ell(R) = \infty$, which is ¬ (d). But we already know that this is equivalent to ¬ (a). □

Proof of (3.120):
This proof is has been taken from the paper *Bilinear Maps on Artinian Modules* by *George M. Bergman* [2012]. It will require several steps:

- In a first step let us assume that b is non-degenerate, then we will eventually prove that L and M are of finite length: Let us denote the sub-modules of L that appear as orthogonal complements under b by

 $$\mathrm{Orc}(L) \;:=\; \left\{ Q^\perp \mid Q \;\leq_{\mathsf{m}}\; M \right\} \;\subseteq\; \mathrm{Subm}(L)$$

 Since L is an artinian module the partially ordered set $(\mathrm{Subm}(L), \subseteq)$ satisfies the DCC. And as $\mathrm{Orc}(L) \subseteq \mathrm{Subm}(L)$ is a subset, we in particular find that $(\mathrm{Orc}(L), \subseteq)$ satisfies the DCC. Likewise orc $(M) \subseteq \mathrm{Subm}(M)$ satisfies the DCC under the partial order $\subseteq$. But by (4.107.(i)) we have a Galois connection

 $$\begin{array}{rcl} \mathrm{Orc}(L) & \longleftrightarrow & \mathrm{Orc}(L) \\ P & \mapsto & P^\top \\ Q^\perp & \hookleftarrow & Q \end{array}$$

 As this correspondence is order-reversing, the DCC of $(\mathrm{Subm}(L), \subseteq)$ is turned into the ACC on $(\mathrm{Subm}(M), \subseteq)$ and vice versa. That is the partially ordered sets $(\mathrm{Subm}(L), \subseteq)$ and $(\mathrm{Subm}(M), \subseteq)$ satisfy *both* ACC and DCC. In particular we know by (0.26) that any chain in $(\mathrm{Subm}(L), \subseteq)$ is finite and can be refined to a maximal chain. Refining $M^\perp = 0 \subset L = 0^\perp$ we get a maximal ascending chain in $\mathrm{Orc}(L)$

 $$0 = P_0 \subset P_1 \subset \ldots \subset P_n = L$$

 Due to the one-to-one correspondence any $P_k \in \mathrm{Orc}(L)$ it is of the form $P_k = Q_k^\perp$ for some sub-module $Q_k \in \mathrm{Orc}(M)$ where we have $Q_k^\perp = P_k$ again. In particular the Q_k for a maximal descending chain in $\mathrm{Orc}(M)$, that is

 $$M = Q_0 \supset Q_1 \supset \ldots \supset Q_n = 0$$

 We will now prove that for any $k \in 1 \ldots n$ the following map is well-defined, bilinear and integral.

But let us take one step at a time

$$b_k \;:\; {}^{P_k}\!\Big/_{P_{k-1}} \times {}^{Q_{k-1}}\!\Big/_{Q_k} \to N \;:\; (u+P_{k-1},\, x+Q_k) \mapsto b(u,x)$$

First of all b_k is well-defined, if $(u+P_{k-1}, x+Q_k) = (v+P_{k-1}, y+Q_k)$ then $v-u \in P_{k-1} = Q_{k-1}^\perp$ and $y-x \in Q_k = P_k^\top$. That is $b(v-u,y) = 0$ for any $y \in Q_{k-1}$ and likewise $b(u,y-x) = 0$ for any $u \in P_k$. But then we can compute

$$\begin{aligned} b(v,y) &= b(v-u,y) + b(u,y) \;=\; b(u,y) \\ &= b(u,y-x) + b(u,x) \;=\; b(u,x) \end{aligned}$$

That is b_k is well-defined and it clearly inherits the bilinearity from b. We also claimed that b_k is *integral*, that is for any $\overline{u} = u + P_{k-1} \in P_k/P_{k-1}$ and any $\overline{x} = x + Q_k \in Q_{k-1}/Q_k$ we have the implication

$$b_k(\overline{u},\overline{x}) \;=\; 0 \quad\Longrightarrow\quad \overline{u} \;=\; 0 \;\text{ or }\; \overline{x} \;=\; 0$$

So let us start with any $u \in P_k = Q_k^\perp$ and $x \in Q_{k-1} = P_{k-1}^\top$. It is clear that for the sub-module $Ru \;\leq_{\mathsf{m}}\; L$ we have

$$\begin{aligned} \big(Ru\big)^\top &= \{\, x \in M \mid \forall\, a \in R : b(au,x) = 0 \,\} \\ &= \{\, x \in M \mid b(u,x) = 0 \,\} \end{aligned}$$

And as $u \in P_k = Q_k^\perp$ we have $Ru \;\subseteq\; Q_k^\perp$ which turns into $Q_k = (Q_k^\perp)^\top \;\subseteq\; (Ru)^\top$. Thus as $Q_k \;\subseteq\; (Ru)^\top$ and as $Q_k \;\subseteq\; Q_{k-1}$ we have

$$Q_k \;\subseteq\; Q_{k-1} \cap \big(Ru\big)^\top \;\subseteq\; Q_{k-1}$$

Thereby $Q_{k-1} \cap (Ru)^\top = P_{k-1}^\top \cap (Ru)^\top = (P_{k-1} + Ru)^\top$ from which we get $Q_{k-1} \cap (Ru)^\top \in \mathrm{Orc}(M)$. However we have chosen the chain $Q_0 \;\supset\; \ldots \;\supset\; Q_{k-1} \;\supset\; Q_k \;\supset\; \ldots \;\supset\; Q_n$ to be maximal in $\mathrm{Orc}(M)$. That is we either have $Q_k = Q_{k-1} \cap (Ru)^\top$ or $Q_{k-1} \cap (Ru)^\top = Q_{k-1}$. In the second case we see $Q_{k-1} \subseteq (Ru)^\top$ and thereby $Ru \subseteq ((Ru)^\top)^\perp \subseteq Q_{k-1}^\perp = Q_{k-1}$ which is $u \in Q_{k-1}$ and thereby $\overline{u} = 0$. So let us assume this is not the case, then necessarily

$$Q_k \;=\; Q_{k-1} \cap \big(Ru\big)^\top$$

If we have $b(u,x) = 0$ then $x \in (Ru)^\top$ and as also $x \in Q_{k-1}$ this implies $x \in Q_k$. But this is $\overline{x} = 0$. Thus we have proved that b_k also is integral. And by (4.107.(iv)) this implies

$$\overline{u} \;\neq\; 0 \;\text{ and }\; \overline{x} \;\neq\; 0 \quad\Longrightarrow\quad \mathrm{ann}(\overline{u}) \;=\; \mathrm{ann}(\overline{x}) \;\in\; \mathrm{Spec}(R)$$

Let $\mathfrak{p}_k := \mathrm{ann}(\overline{u}) = \mathrm{ann}(\overline{x})$ be the common annihilator ideal of all the non-zero elements $\overline{u} \in P_k/P_{k-1}$ and $\overline{x} \in Q_{k-1}/Q_k$ respectively. Then P_k/P_{k-1} (and Q_{k-1}/Q_k) are modules over the ring $R/\mathfrak{p}_k$ by virtue of the scalar multiplication $(a+\mathfrak{p}_k)\overline{u} := a\overline{u}$. But by (3.22) we have the following isomorphy of R-modules

$${}^{R}\!\Big/_{\mathfrak{p}_k} \quad\cong_{\mathsf{m}}\quad R\overline{u} \quad\leq_{\mathsf{m}}\quad {}^{L}\!\Big/_{P_{k-1}}$$

such that $R/\mathfrak{p}_k$ is isomorphic to a sub-module of the artinian module L/P_{k-1}. Hence $R/\mathfrak{p}_k$ is an artinian R-module itself, but this is the same as being an artinian ring (as in a commutative ring sub-modules are ideal). As $\mathfrak{p}_k$ is a prime ideal $R/\mathfrak{p}_k$ is an integral domain and hence a field, by (2.46.(i)). Thus P_k/P_{k-1} is a vector space over $R/\mathfrak{p}_k$. But P_k/P_{k-1} also is artinian, since $P_k \leq_{\mathsf{m}} L$ and L is artinian. But an artinian vector space has finite length, as we have seen in (3.113), resp. (3.119.(vii)). Now we can finally apply (3.118.(iii)) to find

$$\ell(L) \;=\; \sum_{k=1}^{n} \ell\left(P_k \Big/ P_{k-1}\right) \;<\; \infty$$

That is L has finite length, at last. And as the same reasoning holds true for the modules Q_{k-1}/Q_k we find (in complete analogy) that M has finite length, as well.

- For an arbitrary b note that by (4.107.(ii)) b induces a non-degenerate bilinear $\overline{b}$ map of the following form

$$\overline{b} \;:\; L\Big/_{M^\perp} \times M\Big/_{L^\top} \;\to\; N \;:\; \left(u+M^\perp, x+L^\top\right) \;\mapsto\; b(u,x)$$

And as L and M are artinian, so are the residue modules $L/M^\perp$ and $M/L^\top$. Then by the item above we find that $L/M^\perp$ and $M/L^\top$ are of finite length, which was one of the claims.

- As special case of a bilinear map is $t : L \times M \to L \otimes M$ given by $t(u,x) := u \otimes x$. Though it is of no importance to us let us note, that in this case we have $L^\top = \{\, x \in M \mid \forall\, u \in L : u \otimes x = 0 \,\}$, again

$$\overline{t} \;:\; L\Big/_{M^\perp} \times M\Big/_{L^\top} \;\to\; L \otimes M \;:\; \left(u+M^\perp, x+L^\top\right) \;\mapsto\; u \otimes x$$

By the universal property of the tensor product this bilinear map $\overline{t}$ now induces an R-linear map of the following form

$$L\Big/_{M^\perp} \otimes M\Big/_{L^\top} \;\to\; L \otimes M \;:\; \left(u+M^\perp\right) \otimes \left(x+L^\top\right) \;\mapsto\; u \otimes x$$

This map is an isomorphism however: If we denote the canonical projections onto the residue modules by $\varrho_L : L \twoheadrightarrow L/M^\perp : u \mapsto u+M^\perp$ and likewise $\varrho_M : M \twoheadrightarrow M/L^\top : x \mapsto x+L^\top$ then it is clear that $\varrho_L \otimes \varrho_M$ is the inverse map, as it is given to be $(\varrho_L \otimes \varrho_M)(u \otimes x) = \varrho_L(u) \otimes \varrho_M(x) = (u+M^\perp) \otimes (x+L^\top)$. In particular we have the isomorphy of

$$L\Big/_{M^\perp} \otimes M\Big/_{L^\top} \quad \cong_{\mathsf{m}} \quad L \otimes M$$

But in the item above we have proved that both $L/M^\perp$ and $M/L^\top$ are modules of finite length. And hence $L \otimes M$ is a module of finite length, too as by (3.155.(iii)) we have

$$\begin{aligned} \ell(L \otimes M) \;&=\; \ell\left(L\Big/_{M^\perp} \otimes M\Big/_{L^\top}\right) \\ &\leq\; \ell\left(L\Big/_{M^\perp}\right) + \ell\left(M\Big/_{L^\top}\right) \;<\; \infty \end{aligned}$$

□

Proof of (4.70):

(i) For any α and $\beta \in \mathrm{Asc}(r,n)$ let us denote the following map of the form $D_{\alpha,\beta} : \mathrm{mat}_n(R) = (R^n)^n \to R$, defined by

$$D_{\alpha,\beta}(A) \;:=\; \det\big(A[\alpha \mid \beta]\big) \cdot \det\big(A[\widehat{\alpha} \mid \widehat{\beta}]\big)$$

In a first step we will show that $D_{\alpha,\beta}$ is multi-linear. However we will do this for the first column of A only, as the other columns are just more notational fuzz. That is for any $a \in R$ and any $a_1, a_2, \ldots a_n \in R$ and any $b_1 \in R^n$ we need to show the properties

$$\begin{aligned} D_{\alpha,\beta}(a\,a_1, a_2, \ldots, a_n) &= a\,D_{\alpha,\beta}(a_1, a_2, \ldots, a_n) \\ D_{\alpha,\beta}(a_1 + b_1, a_2, \ldots, a_n) &= D_{\alpha,\beta}(a_1, a_2, \ldots, a_n) + \\ & \quad D_{\alpha,\beta}(b_1, a_2, \ldots, a_n) \end{aligned}$$

To further complicate things we denote $x' := (x_{\alpha(1)}, \ldots, x_{\alpha(r)}$ for any $x = (x_1, x_2, \ldots, x_n) \in R^n$. The scalar multiplicativity is quite obvious: If $1 \in S(\beta)$ then aa'_1 appears as the first column of $A[\alpha \mid \beta]$ and as the determinant is multi-linear we call pull the a in front. That is

$$\det\big((aa_1\, a_2\, \ldots\, a_n)[\alpha \mid \beta]\big) \;=\; a\det\big((a_1\, a_2\, \ldots\, a_n)[\alpha \mid \beta]\big)$$

And in this case $1 \in S(\beta)$ we also get $1 \notin S(\widehat{\beta})$ such that first column of A is scratched in $A[\widehat{\alpha} \mid \widehat{\beta}]$ and with it a. Therefore we then get

$$\det\big((aa_1\, a_2\, \ldots\, a_n)[\widehat{\alpha} \mid \widehat{\beta}]\big) \;=\; \det\big((a_1\, a_2\, \ldots\, a_n)[\widehat{\alpha} \mid \widehat{\beta}]\big)$$

If $1 \notin S(\beta)$ then $1 \in S(\widehat{\beta})$ so in any case the first column of A is scratched from one matrix but not from the other. So in both cases we find the first equation, needed:

$$D_{\alpha,\beta}(a\,a_1, a_2, \ldots, a_n) \;=\; a\,D_{\alpha,\beta}(a_1, a_2, \ldots, a_n)$$

Next we need to verify the additivity of $D_{\alpha,\beta}$ - to do this we need to introduce some matrices: First of all $A := (a_1\, a_2\, \ldots\, a_n)$ then $B_0 := (b_1\, 0\, \ldots\, 0)$ and lastly $B := (b_1\, a_2\, \ldots\, a_n)$. Using these we need to verify (compare this to the second equation above)

$$D_{\alpha,\beta}(A + B_0) \;=\; D_{\alpha,\beta}(A) + D_{\alpha,\beta}(B)$$

Again we need to distinguish two cases, beginning with $1 \in S(\beta)$. In this case $(A + B_0)[\alpha \mid \beta]$ contains $a'_1 + b'_1$ as the first column and as the determinant still is multi-linear we can pull out that sum:

$$\det\big((A + B_0)\,[\alpha \mid \beta]\,\big) \;=\; \det\big(A\,[\alpha \mid \beta]\,\big) + \det\big(B\,[\alpha \mid \beta]\,\big)$$

Note that in case $1 \in S(\beta)$ we have $1 \notin S(\widehat{\beta})$ again such that the first column of $A + B_0$ is scratched in $(A + B_0)[\widehat{\alpha} \mid \widehat{\beta}]$ entirely. Thus B_0 does not affect the result at all. And as A and B only differ in the first column, we also have $A[\widehat{\alpha} \mid \widehat{\beta}] = B[\widehat{\alpha} \mid \widehat{\beta}]$ such that

$$\det\Big((A + B_0)\,\Big[\widehat{\alpha} \mid \widehat{\beta}\Big]\Big) \;=\; \det\Big(A\,\Big[\widehat{\alpha} \mid \widehat{\beta}\Big]\Big) \;=\; \det\Big(B\,\Big[\widehat{\alpha} \mid \widehat{\beta}\Big]\Big)$$

If we combine these two equations and use the law of distibutivity we find the second equation

needed (in case $1 \in S(\beta)$)

$$\begin{aligned}
& D_{\alpha,\beta}(A + B_0) \\
= \;& \det\left((A + B_0)\,[\alpha \mid \beta]\right) \cdot \det\left((A + B_0)\left[\widehat{\alpha} \mid \widehat{\beta}\right]\right) \\
= \;& \left(\det\left(A\,[\alpha \mid \beta]\right) + \det\left(B\,[\alpha \mid \beta]\right)\right) \cdot \det\left(A\left[\widehat{\alpha} \mid \widehat{\beta}\right]\right) \\
= \;& D_{\alpha,\beta}(A) + \det\left(B\,[\alpha \mid \beta]\right) \cdot \det\left(A\left[\widehat{\alpha} \mid \widehat{\beta}\right]\right) \\
= \;& D_{\alpha,\beta}(A) + \det\left(B\,[\alpha \mid \beta]\right) \cdot \det\left(B\left[\widehat{\alpha} \mid \widehat{\beta}\right]\right) \\
= \;& D_{\alpha,\beta}(A) + D_{\alpha,\beta}(B)
\end{aligned}$$

If $1 \notin S(\beta)$ then $1 \in S(\widehat{\beta})$ so in any case the first column of $A + B_0$ is scratched from the first matrix but not from the second. In complete analogy to the above we arrive at

$$D_{\alpha,\beta}(A + B_0) \;=\; D_{\alpha,\beta}(A) + D_{\alpha,\beta}(B)$$

Altogether for any α, $\beta \in \mathrm{Asc}(r,n)$ the map $D_{\alpha,\beta}$ is multi-linear. Hence any R-linear combination of these maps is multi-linear, such as

$$D_\alpha(A) \;:=\; \sum_{\beta \in \mathrm{Asc}(r,n)} (-1)^{|\alpha|+|\beta|} D_{\alpha,\beta}(A)$$

Note that $D_\alpha(A)$ is precisely the expression of which we need to show that $D_\alpha(A) = \det(A)$. In a next step we will prove that D_α is alternating: That is whenever A has two equal columns, such as $a_p = a_q$ for some $p < q \in 1 \ldots n$ then we need $D_\alpha(A) = 0$. If both p and $q \in S(\beta)$ then $A[\alpha \mid \beta]$ contains a'_p and a'_q which are equal and hence $\det(A[\alpha \mid \beta]) = 0$. Hence all the summands of D_α in which $\{\, p, q \,\} \subseteq S(\beta)$ vanish. The same is true if $\{\, p, q \,\} \subseteq S(\widehat{\beta})$ that is if $p \notin S(\beta)$ and $q \notin S(\beta)$. Thus we may split D_α into the distinct sums

$$\begin{aligned}
D_\alpha(A) \;=\; & \sum_{p \in S(\beta),\, q \notin S(\beta)} (-1)^{|\alpha|+|\beta|} D_{\alpha,\beta}(A) + \\
& \sum_{p \notin S(\beta),\, q \in S(\beta)} (-1)^{|\alpha|+|\beta|} D_{\alpha,\beta}(A)
\end{aligned}$$

That is these two distinct sums run over the following subsets of $\mathrm{Asc}(r,n)$

$$\begin{aligned}
P \;&:=\; \{\, \beta \in \mathrm{Asc}(r,n) \mid p \in S(\beta),\; q \notin S(\beta) \,\} \\
Q \;&:=\; \{\, \beta \in \mathrm{Asc}(r,n) \mid p \notin S(\beta),\; q \in S(\beta) \,\}
\end{aligned}$$

If $\beta \in P$ then let us define $\beta' \in \mathrm{Asc}(r,n)$ such that p is replaced by q. That is β' is the uniquely determined ascending of indexes chain with

$$S(\beta') \;=\; (S(\beta) \setminus \{\, p \,\}) \cup \{\, q \,\}$$

Note that $\beta \mapsto \beta'$ is a bijection from P to Q, as the inverse map is given by replacing q by p. Also

it is clear, that $|\beta'| = |\beta| - p + q$, i.e.

$$|\beta'| - |\beta| \;=\; q - p$$

Now what does β' look like? Let $i, j \in 1 \dots n$ such that $p = \beta(i)$ and $q = \beta'(j)$. Then we see that β' with $d := j - i \geq 1$ is precisely the following chain of indexes (in ascending order)

$$\begin{array}{ccc}
\beta'(1) & = & \beta(1) \\
\vdots & & \vdots \\
\beta'(i-1) & = & \beta(i-1) \\
\hline
 & & \beta(i) = p \\
\beta'(i) & = & \beta(i+1) \\
\vdots & & \vdots \\
\beta'(i+d-1) & = & \beta(i+d) \\
\beta'(i+d) = q & & \\
\hline
\beta'(i+d+1) & = & \beta(i+d+1) \\
\vdots & & \vdots \\
\beta'(r) & = & \beta(r)
\end{array}$$

That is: The middle section of β' is a shifted version of the middle section of β and hence we can decompose $A[\alpha \mid \beta]$ into three blocks

$$\begin{aligned}
A'_L &:= \begin{pmatrix} | & & | \\ a'_{\beta(1)} & \dots & a'_{\beta(i-1)} \\ | & & | \end{pmatrix} \\
A'_S &:= \begin{pmatrix} | & & | \\ a'_{\beta(i+1)} & \dots & a'_{\beta(i+d)} \\ | & & | \end{pmatrix} \\
A'_R &:= \begin{pmatrix} | & & | \\ a'_{\beta(i+d+1)} & \dots & a'_{\beta(r)} \\ | & & | \end{pmatrix}
\end{aligned}$$

That is $A[\alpha \mid \beta] = (A'_L\, a'_p\, A'_S\, A'_R)$ (recall that the prime denotes the scratching of rows due to α) and likewise $A[\alpha \mid \beta'] = (A'_L\, A'_S\, a'_q\, A'_R)$. But as $a'_p = a'_q$ we see that we get $A[\alpha \mid \beta']$ by permuting the columns of $A[\alpha \mid \beta]$ with the cycle ζ^{-1} where $\zeta = (i\; i+1\; \dots\; i+d)$ and hence

$$A[\alpha \mid \beta'] \;=\; A[\alpha \mid \beta]\, P_\zeta^{-1}$$

As $\zeta \in S_r$ is a cycle of length $d+1$ we have $\operatorname{sgn}(\zeta) = d$ and hence $\det(P_\zeta^{-1}) = \operatorname{sgn}(\zeta)^{-1} = (-1)^{-d} = (-1)^d$. Altogether

$$\det\left(A[\alpha \mid \beta']\right) \;=\; (-1)^d \det\left(A[\alpha \mid \beta]\right)$$

Let us summarize: Since we get to β' by shifting $d+1$ elements of β the determinant of $A[\alpha \mid \beta']$

gains the factor $(-1)^d$. The same consideration applies when we compare $\widehat{\beta}'$ to $\widehat{\beta}$. As $p \in S(\beta)$ we have $p \notin S(\beta')$ and then again $p \in S(\widehat{\beta}')$. For the same reason $q \notin S(\widehat{\beta}')$. Only the indexes of $\widehat{\beta}$ from p to q are shifted. But how many are there? First of all there are $q-p+1$ numbers in between, but of these d belonged to β (including p). Thus we have to shift $q-p-d$ indexes to turn $\widehat{\beta}$ into $\widehat{\beta}'$ and therefore

$$\det\left(A[\widehat{\alpha} \mid \widehat{\beta}']\right) \;=\; (-1)^{q-p-d-1} \det\left(A[\widehat{\alpha} \mid \widehat{\beta}]\right)$$

Altogether

$$\begin{aligned} D_{\alpha,\beta'}(A) &= \det\left(A[\alpha \mid \beta']\right) \cdot \det\left(A[\widehat{\alpha} \mid \widehat{\beta}']\right) \\ &= (-1)^d \det\left(A[\alpha \mid \beta]\right) \cdot (-1)^{q-p-d-1} \det\left(A[\widehat{\alpha} \mid \widehat{\beta}]\right) \\ &= (-1)^{q-p-1} \det\left(A[\alpha \mid \beta]\right) \cdot \det\left(A[\widehat{\alpha} \mid \widehat{\beta}]\right) \\ &= -(-1)^{q-p} D_{\alpha,\beta}(A) \end{aligned}$$

That is every $\beta \in P$ has a partner $\beta' \in Q$ such that the respective summands in D_α cancel each other. Formally we may compute

$$\begin{aligned} & \sum_{\beta \in Q} (-1)^{|\alpha|+|\beta|} D_{\alpha,\beta}(A) \\ = \; & \sum_{\beta \in P} (-1)^{|\alpha|+|\beta'|} D_{\alpha,\beta'}(A) \\ = \; & -\sum_{\beta \in P} (-1)^{|\alpha|+|\beta|-p+q} (-1)^{q-p} D_{\alpha,\beta}(A) \\ = \; & -\sum_{\beta \in P} (-1)^{|\alpha|+|\beta|} D_{\alpha,\beta}(A) \end{aligned}$$

In a final step we will prove $D_\alpha(\mathbb{1}_n) = 1$. To do this we will first show $\det(\mathbb{1}_n[\alpha \mid \beta]) = \delta_{\alpha,\beta}$. By the definition of the determinant we can evaluate this explicitly

$$\begin{aligned} \det(\mathbb{1}_n[\alpha \mid \beta]) &= \sum_{\sigma \in S_r} \operatorname{sgn}(\sigma) \prod_{i=1}^{r} \operatorname{ent}_{i,\sigma(i)}(\mathbb{1}_n[\alpha \mid \beta]) \\ &= \sum_{\sigma \in S_r} \operatorname{sgn}(\sigma) \prod_{i=1}^{r} \delta_{\alpha(i),\beta\sigma(i)} \\ &= \sum_{\sigma \in S_r} \operatorname{sgn}(\sigma) \begin{cases} 1 \text{ if } \alpha = \beta\sigma \\ 0 \text{ if } \alpha \neq \beta\sigma \end{cases} \end{aligned}$$

However if $\alpha = \beta\sigma$ then in particular $S(\alpha) = S(\beta)$ and hence $\alpha = \beta$. That is we have $\det(\mathbb{1}_n[\alpha \mid \beta]) = 0$ whenever $\alpha \neq \beta$. In case $\alpha = \beta$ we have $\alpha = \beta\sigma$ if and only if $\sigma = \mathbb{1}$ which features $\operatorname{sgn}(\mathbb{1}) = 1$. Thus in case $\alpha = \beta$ we have $\det(\mathbb{1}_n[\alpha \mid \beta]) = 1$. In this case we also have $\widehat{\alpha} = \widehat{\beta}$ such that

$$\begin{gathered} D_{\alpha,\beta}(\mathbb{1}_n) \;=\; \delta_{\alpha,\beta} \\ \Longrightarrow \quad D_\alpha(\mathbb{1}_n) \;=\; \sum_{\beta \in \operatorname{Asc}(r,n)} (-1)^{|\alpha|+|\beta|} \delta_{\alpha,\beta} \;=\; (-1)^{2|\alpha|} \;=\; 1 \end{gathered}$$

In the three steps above we have *finally* shown, that D_α is an alternating, multi-linear map, so by lemma (4.55.(iv)) we now find

$$D_\alpha(A) \;=\; D_\alpha(\mathbb{1}_n)\cdot\det(A) \;=\; \det(A)$$

Thus we have proved the first formula in the Laplace expansion theorem. But as $A^*[\alpha \mid \beta] = A[\beta \mid \alpha]^*$ (4.83.(i)) and the determinant is invariant under transposition (4.55.(i)) we find $D_{\alpha,\beta}(A^*) = D_{\beta,\alpha}(A)$. Thus the second formula in the Laplace expansion theorem follows by applying the first formula to the transpose matrix A^*.

(ii) Now consider the product matrix $C = AB\mathrm{mat}_{k,n}(R)$, that is the (i,j)-th entry of C is $c_{i,j} = \langle \mathrm{row}_i(A), \mathrm{col}_j(B)\rangle$. Then for any $p, q \in 1\ldots r$ the (p,q)-th entry of $C[\alpha,\gamma]$ is

$$\begin{aligned}\mathrm{ent}_{p,q}(C[\alpha,\gamma]) &= \mathrm{ent}_{\alpha(p),\gamma(q)}(C)\\ &= \langle \mathrm{row}_{\alpha(p)}(A), \mathrm{col}_{\gamma(q)}(B)\rangle\\ &= \sum_{\beta=1}^{m} a_{\alpha(p),\beta}\, b_{\beta,\gamma(q)}\end{aligned}$$

We now evaluate the determinant of $C[\alpha,\gamma]$ explicitly, using nothing but the definition of the determinant, which is

$$\begin{aligned}&\det(C[\alpha,\gamma])\\ =\;& \sum_{\sigma\in S_r}\mathrm{sgn}(\sigma)\prod_{p=1}^{r}\mathrm{ent}_{p,\sigma(p)}(C[\alpha,\gamma])\\ =\;& \sum_{\sigma\in S_r}\mathrm{sgn}(\sigma)\prod_{p=1}^{r}\left(\sum_{\beta=1}^{m} a_{\alpha(p),\beta}\, b_{\beta,\gamma\sigma(p)}\right)\\ =\;& \sum_{\sigma\in S_r}\mathrm{sgn}(\sigma)\sum_{\beta(1)=1}^{m}\cdots\sum_{\beta(r)=1}^{m}\prod_{p=1}^{r} a_{\alpha(p),\beta(p)}\, b_{\beta(p),\gamma\sigma(p)}\\ =\;& \sum_{\beta\in(1\ldots m)^r}\sum_{\sigma\in S_r}\mathrm{sgn}(\sigma)\prod_{p=1}^{r} a_{\alpha(p),\beta(p)}\, b_{\beta(p),\gamma\sigma(p)}\\ =\;& \sum_{\beta\in(1\ldots m)^r}\prod_{p=1}^{r} a_{\alpha(p),\beta(p)}\sum_{\sigma\in S_r}\mathrm{sgn}(\sigma)\prod_{p=1}^{r} b_{\beta(p),\gamma\sigma(p)}\\ =\;& \sum_{\beta\in(1\ldots m)^r}\prod_{p=1}^{r} a_{\alpha(p),\beta(p)}\det\begin{pmatrix} b_{\beta(1),\gamma\sigma(1)} & \cdots & b_{\beta(1),\gamma\sigma(r)}\\ \vdots & \ddots & \vdots\\ b_{\beta(r),\gamma\sigma(1)} & \cdots & b_{\beta(r),\gamma\sigma(r)}\end{pmatrix}\\ =\;& \sum_{\beta\in(1\ldots m)^r}\prod_{p=1}^{r} a_{\alpha(p),\beta(p)}\det\big(B[\beta \mid \gamma]\big)\end{aligned}$$

If $\beta(p) = \beta(q)$ for some $p \neq q \in 1\ldots r$ then the p-th and q-th rows of the matrix $B[\beta \mid \gamma]$ are the same and hence its determinant vanishes. Thus this sum breaks down to the terms in which $\beta : 1\ldots r \hookrightarrow 1\ldots m$ is injective. There is an equivalence relation on the set of injections from $1 \to r$ to $1\ldots m$ however, by letting $\beta \sim \beta'$ if and only if $\beta(1\ldots r) = \beta'(1\ldots r)$. Every equivalence

class $[\beta]$ has a uniquely determined representative $\beta \in \mathrm{Asc}(r,m)$ and the class then is

$$[\beta] \;=\; \{\, \beta\varrho \mid \varrho \in S_r \,\}$$

Thus we may split the sum over all (injective) $\beta \in (1\ldots m)^r$ into a sum over $\beta \in \mathrm{Asc}(r,m)$ and a sum over all $\varrho \in S_r$

$$\det(C[\alpha,\gamma]) \;=\; \sum_{\beta\in\mathrm{Asc}(r,m)} \sum_{\varrho\in S_r} \prod_{p=1}^{r} a_{\alpha(p),\beta\varrho(p)}\, \det\big(B[\beta\varrho \mid \gamma]\big)$$

Now we see that for any fixed $\beta \in \mathrm{Asc}(r,m)$ the matrices in the above term are just different versions of the same matrix subjected to a permutation of rows $B[\beta\varrho \mid \gamma] = P_\varrho\, B[\beta \mid \gamma]$ In particular their determinants are just $\mathrm{sgn}(\varrho)$ times the determinant of the original matrix. Using this the determinant of $C[\alpha,\gamma]$ can finally be written in the desired form

$$\begin{aligned}
\det(C[\alpha,\gamma]) \;&=\; \sum_{\beta\in\mathrm{Asc}(r,m)} \sum_{\varrho\in S_r} \prod_{p=1}^{r} a_{\alpha(p),\beta\varrho(p)} \mathrm{sgn}(\varrho)\, \det\big(B[\beta \mid \gamma]\big) \\
&=\; \sum_{\beta\in\mathrm{Asc}(r,m)} \det\big(B[\beta \mid \gamma]\big) \sum_{\varrho\in S_r} \mathrm{sgn}(\varrho) \prod_{p=1}^{r} a_{\alpha(p),\beta\varrho(p)} \\
&=\; \sum_{\beta\in\mathrm{Asc}(r,m)} \det\big(B[\beta \mid \gamma]\big)\, \det\big(A[\alpha \mid \beta]\big)
\end{aligned}$$

□

Proof of (4.72):

(i) As the column rank of A has been defined, as the maximal number of linearly independent columns of A it is clear that c-rank$(A) \le n$. For any $j \in 1\ldots n$ let us now abbreviate $c_j := \mathrm{col}_j(A) \in R^m$ the j-th column of A. As $R^m = \mathrm{Lh}\{\, e_1, e_2, \ldots, e_m \,\}$ is generated by m elements lemma (3.99.(i)) tells us, that - whenever $J \subseteq 1\ldots n$ with $\#J \ge m+1$ - the set $\{\, c_j \mid j \in J \,\}$ is linearly dependent. In particular the number of linearly independent columns c_j cannot exceed m, that is c-rank$A \le m$, as well.

For the same property of the row-rank just consider the transpose matrix A^*. As this satisfies r-rank(A) = c-rank$(A^*) \le \min\{\, m,n \,\}$ the statement is already proved, as well.

The same reasoning can be used to prove c-rank$(A) \le$ i-rank(A): By definition of the vector-matrix multiplication we have $Ax = x_1c_1 + \cdots + x_nc_n \in R^m$ for any $x \in R^n$ and thereby $\mathrm{im}(A) = \mathrm{Lh}\{\, c_1, \ldots, c_n \,\}$. In particular $c_J := \{\, c_j \mid j \in J \,\} \subseteq \mathrm{im}(A)$ for any $J \subseteq 1\ldots n$. Now pick up a generating set $\{\, x_1, \ldots, x_r \,\} \subseteq \mathrm{im}(A)$ of $\mathrm{im}(A)$ such that $r = \mathrm{rank}(\mathrm{im}(A)) =$ i-rank(A). If $J \subseteq 1\ldots n$ such that c_J is linearly independent, then necessarily $\#J \le r$, by (3.99.(i)) again. And as c-rank$(A) = \#J$ for some $J \subseteq 1\ldots n$ this means c-rank$(A) \le r = \mathrm{rank}(\mathrm{im}(A)) =$ i-rank(A).

(i) **Remark:** In the proof of (i) we used the very intricate lemma (3.99.(i)) which in turn uses Hilbert's basis theorem and the theory of noetherian modules. In the case of a field R, this argument can be replaced by (3.66.(vii)) which likewise implies that $\#J \le \dim(R^m) = m$.

(ii) Let us abbreviate $B_j := \mathrm{col}_j(B)$ and suppose for some $J \subseteq 1\ldots n$ the vectors $\{\, B_j \mid j \in J \,\}$ are

linearly dependent. That is we have

$$\sum_{j\in J} a_i B_j \;=\; 0$$

for some $a_j \in R$ that are not all $= 0$. But since A is linear this already implies, that $\{\, AB_j \mid j \in J \,\}$ is linearly dependent as well, since

$$\sum_{j\in J} a_i AB_j \;=\; A\left(\sum_{j\in J} a_i B_j\right) \;=\; A(0) \;=\; 0$$

Negating the statement we find: If $\{\, AB_j \mid j \in J \,\}$ is linearly independent then $\{\, B_j \mid j \in J \,\}$ has already been linearly independent. Recall that the AB_1, AB_2 to AB_n are precisely the columns of AB. Hence

$$\text{c-rank}(AB) \;\leq\; \text{c-rank}(B)$$

Recall that $(AB)^* = B^*A^*$ since R is commutative. Such that, going to transpose matrices, we find the following inequality from this

$$\text{r-rank}(AB) \;=\; \text{c-rank}(B^*A^*) \;\leq\; \text{c-rank}(A^*) \;=\; \text{r-rank}(A)$$

(iii) Let us abbreviate $A' := A[\alpha \mid \beta]$ and $q := \text{c-rank}(A')$. For ease of notation let us also assume that $\text{col}_1(A')$ to $\text{col}_q(A') \in R^m$ are linearly independent columns of A'. We now define the map $P_\alpha : R^m \to R^r$ by virtue of $P_\alpha(x) := x'$ where for $x = (x_1, \ldots, x_m) \in R^m$ we let $x' := (x_{\alpha(1)}, \ldots, x_{\alpha(r)}) \in R^r$. Then it is clear, that

$$\text{col}_j(A') \;=\; P_\alpha\left(\text{col}_{\beta(j)}(A)\right)$$

for any $j \in 1 \ldots s$. We will now prove that $\text{col}_{\beta(1)}(A)$ to $\text{col}_{\beta(q)}(A)$ are linearly independent. To do this let us assume there was some relation between these vectors

$$\sum_{j=1}^{q} a_j \,\text{col}_{\beta(j)}(A) \;=\; 0$$

As the projection P_α is R-linear this would also yield a relation between the vectors $\text{col}_1(A')$ to $\text{col}_q(A')$, since

$$\begin{aligned} 0 \;&=\; P_\alpha\left(\sum_{j=1}^{q} a_j \,\text{col}_{\beta(j)}(A)\right) \\ &=\; \sum_{j=1}^{q} a_j \, P_\alpha\left(\text{col}_{\beta(j)}(A)\right) \\ &=\; \sum_{j=1}^{q} a_j \,\text{col}_j(A') \end{aligned}$$

But since these are linearly independent by assumption, this means $a_j = 0$ for any $j \in 1 \ldots q$. But this is precisely the linear independence of the $\text{col}_{\beta(j)}(A)$. That is A contains at least q linearly

independent columns and hence we find

$$\text{c-rank}(A') \;=\; q \;<\; \text{c-rank}(A)$$

For the row-rank we simply take to the transpose matrix: Note that $A[\alpha \mid \beta]^* = A^*[\beta \mid \alpha]$ and use the inequality we have just shown for the column-rank

$$\begin{aligned}\text{r-rank}(A) \;&=\; \text{c-rank}(A^*) \;\geq\; \text{c-rank}(A^*[\beta \mid \alpha]) \\ &=\; \text{c-rank}(A[\alpha \mid \beta]^*) \;=\; \text{r-rank}(A[\alpha \mid \beta])\end{aligned}$$

(v) Define $\alpha \in \text{Asc}(r,m)$ by $\alpha(i) = i$ for any $i \in 1 \ldots r$ and consider the submatrix $A' := A[\alpha \mid \mu]$ of A. That is $a'_{i,i} = a_{\alpha(i),\mu(i)} = a_{i,\mu(i)} \neq 0$ and $a'_{i,j} = a_{\alpha(i),\mu(j)} = a_{i,\mu(j)}$. If now $j < i$, then $\mu(j) < \mu(i)$ such that the assumption on A then yields $a'_{i,j} = 0$. Altogether A' is a square, upper triangular matrix non-zero entries on the diagonal

$$A' \;=\; \begin{pmatrix} a_{1,\mu(1)} & a_{1,\mu(2)} & \cdots & a_{1,\mu(r)} \\ 0 & a_{2,\mu(2)} & \cdots & a_{2,\mu(r)} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & a_{r,\mu(r)} \end{pmatrix}$$

We will now prove, that in this case $\text{r-rank}(A') = r$. That is we need to show that all the r rows of A' are linearly independent. Suppose

$$\sum_{i=1}^{r} a_i \,\text{row}_i(A') \;=\; 0$$

then we have to show that all the a_i are zero. We start with a_r and use induction down to a_1. Since the sum in R^r is zero, so are all its components, in particular

$$0 \;=\; \left[\sum_{i=1}^{r} a_i \,\text{row}_i(A')\right]_r \;=\; \sum_{i=1}^{r} a_i \,a'_{r,i} \;=\; a_r \,a'_{r,r}$$

In the last step we used that $a'_{r,i} = 0$ for any $i < r$. But we also have $a'_{r,r} \neq 0$ which means - since R is an integral domain - that $a_r = 0$. Now suppose we already had $a_r = a_{r-1} = \cdots = a_{k+1} = 0$. Then we want to show, that $a_k = 0$, as well. To do this compute

$$0 \;=\; \left[\sum_{i=1}^{r} a_i \,\text{row}_i(A')\right]_k \;=\; \sum_{i=1}^{r} a_i \left[\text{row}_i(A')\right]_k \;=\; \sum_{i=1}^{k} a_i \left[\text{row}_i(A')\right]_k$$

by induction hypothesis. As before $a'_{k,i} = 0$ for any $i < k$ such that this sum also boils down to a single term

$$0 \;=\; \sum_{i=1}^{k} a_i \left[\text{row}_i(A')\right]_k \;=\; \sum_{i=1}^{k} a_i \,a'_{k,i} \;=\; a_k \,a'_{k,k}$$

Again, as $a'_{k,k} \neq 0$ and R is an integral domain we conclude $a_k = 0$. Thus we find $a_i = 0$ for any $i \in 1 \ldots r$, which means that the rows of A' are linearly independent and therefore $\text{r-rank}(A') = r$.

In exactly the same way we can prove that c-rank$(A') = 0$, in this case we would start with $a_1 = 0$ and use induction up to $a_r = 0$. But as A' is a submatrix of A item (iii) tells us, that

$$\begin{aligned} \text{c-rank}(A) &\geq \text{c-rank}(A') = r \\ \text{r-rank}(A) &\geq \text{r-rank}(A') = r \end{aligned}$$

On the other hand the assumption on A includes $\text{row}_i(A) = 0$ for any $i > r$. That is in truth A is of the following form

$$A = \begin{pmatrix} \text{---} & \text{row}_1(A'') & \text{---} \\ & \vdots & \\ \text{---} & \text{row}_r(A'') & \text{---} \\ 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{pmatrix}$$

for some $A'' \in \text{mat}_{r,n}(R)$. As the zero-rows clearly at the bottom do neither contribute to the column-rank nor the row-rank of A we have c-rank$(A) =$ c-rank(A'') and also r-rank$(A) =$ r-rank(A''). It is clear that r-rank$(A'') \leq r$ such that

$$r = \text{r-rank}(A') \leq \text{r-rank}(A) = \text{r-rank}(A'') \leq r$$

and we finally get r-rank$(A) = r$. But by (i) we also have c-rank$(A'') \leq r$, such that the same argument holds true for the column-rank and we also find c-rank$(A) = r$ according to

$$r = \text{c-rank}(A') \leq \text{c-rank}(A) = \text{c-rank}(A'') \leq r$$

(vi) Let us first prove c-rank$(A) =$ free(M): To do this consider some set $J \subseteq 1 \dots n$ of indexes, such that $\{ c_j \mid j \in J \}$ is linearly independent, but for any $k \in 1 \dots n \setminus J$ the set $\{ c_j \mid j \in J \} \cup c_k$ is linearly dependent. Then $L := \{ c_j \mid j \in J \}$ and $X := \{ c_k \mid k \in 1 \dots n \setminus J \}$ satisfy the assumptions of corollary (3.102.(v)). Therefore we find

$$\text{c-rank}(A) = \#J = \text{free}(M) \leq \text{rank}(M) = \text{i-rank}(A)$$

The proof of r-rank$(A) =$ free(N) is just the same: In this case we pick up $I \subseteq 1 \dots m$ such that $L := \{ r_i \mid i \in I \}$ is linearly independent such that for any $k \in 1 \dots m \setminus I$ the set $L \cup \{ r_k \}$ is linearly dependent. Then (3.102.(v)) again implies

$$\text{r-rank}(A) = \#I = \text{free}(N)$$

(vi) It remains to prove that c-rank$(A) =$ r-rank(A). Let us abbreviate the j-th column (where $j \in 1 \dots n$) of A by $c_j := \text{col}_j(A) \in R^m$. If now $r = \text{c-rank}(A)$ then there is some $\beta \in \text{Asc}(r, n)$ such that

$$\left\{ c_{\beta(i)} \mid i \in 1 \dots r \right\} \subseteq R^m$$

is R-linearly independent. Let $E := \text{QUOT}(R)$ be the quotient field of R, then by (3.63) this set is

E-linearly independent as well. Thus it even is a basis of

$$U \;:=\; \mathrm{Lh}_E\{\, c_{\beta(i)} \mid i \in 1 \dots r \,\} \quad \leq_{\mathrm{v}} \quad E^m$$

By assumption any other c_k is R-linearly dependent on this set, that is for any $k \in 1 \dots n$ there are coefficients $t_{i,k} \in R$ such that

$$c_k \;=\; \sum_{i=1}^{r} t_{i,k}\, c_{\beta(i)}$$

We will later use the matrix of these coefficients $T := (t_{i,k}) \in \mathrm{mat}_{r,n}(R)$. In particular it is clear that U even is the entire column space of A

$$U \;=\; \mathrm{Lh}_E\{\, c_j \mid j \in 1 \dots n \,\} \quad \leq_{\mathrm{v}} \quad E^m$$

Let us define the submatrix $A' \in \mathrm{mat}_{m,r}(R)$ of A that is made of exactly these r linearly independent columns of A, that is

$$\begin{aligned} A' \;&:=\; \begin{pmatrix} | & | & & | \\ c_{\beta(1)} & c_{\beta(2)} & \dots & c_{\beta(r)} \\ | & | & & | \end{pmatrix} \\ &=\; \begin{pmatrix} a_{1,\beta(1)} & a_{1,\beta(2)} & \dots & a_{1,\beta(r)} \\ a_{2,\beta(1)} & a_{2,\beta(2)} & \dots & a_{2,\beta(r)} \\ \vdots & \vdots & & \vdots \\ a_{m,\beta(1)} & a_{m,\beta(2)} & \dots & a_{m,\beta(r)} \end{pmatrix} \end{aligned}$$

Looking at proposition (4.20) we see that $X = A$ and $Y = A'$ such that $A = A'T$. But on the other hand we can compute

$$A \;=\; A'T \;=\; \begin{pmatrix} \text{——} & T^*\mathrm{row}_1(A') & \text{——} \\ \text{——} & T^*\mathrm{row}_2(A') & \text{——} \\ & \vdots & \\ \text{——} & T^*\mathrm{row}_m(A') & \text{——} \end{pmatrix}$$

Thereby for any $p \in 1 \dots m$

$$\begin{aligned} T^*\mathrm{row}_p(A') \;&=\; \begin{pmatrix} t_{1,1} & \dots & t_{r,1} \\ \vdots & & \vdots \\ t_{1,n} & \dots & t_{r,n} \end{pmatrix} \begin{pmatrix} a_{p,\beta(1)} \\ \vdots \\ a_{p,\beta(r)} \end{pmatrix} \\ &=\; \begin{pmatrix} \sum_{i=1}^{r} t_{i,1} a_{p,\beta(i)} \\ \vdots \\ \sum_{i=1}^{r} t_{i,n} a_{p,\beta(i)} \end{pmatrix} \\ &=\; \sum_{i=1}^{r} a_{p,\beta(i)} \begin{pmatrix} t_{i,1} \\ \vdots \\ t_{i,n} \end{pmatrix} \end{aligned}$$

$$= \sum_{i=1}^{r} a_{p,\beta(i)}\, \mathrm{row}_i(T)$$

In particular we see that for any $p \in 1 \dots m$ the p-th row of A is a R-linear combination of the r rows of T

$$\mathrm{row}_p(A) \;=\; T^* \mathrm{row}_p(A') \;\in\; \mathrm{Lh}_E\{\, \mathrm{row}_i(T) \mid i \in 1 \dots r \,\}$$

Hereby the row space of T (as a subspace of E^n) is generated by r elements and hence is at most r-dimensional. Therefore there can be at most r E-linearly independent rows $\mathrm{row}_p(A)$ of A. But if any $r+1$ rows of A are E-linearly dependent by (3.63) again, they are R-linearly dependent already. And this finally means

$$\text{r-rank}(A) \;\leq\; r \;=\; \text{c-rank}(A)$$

Note that this inequality has been established for any matrix A of any size. Thus it also holds true for $B := A^*$. And with this we also find the converse inequality

$$\text{c-rank}(A) \;=\; \text{r-rank}(B) \;\leq\; \text{c-rank}(B) \;=\; \text{r-rank}(A)$$

(iv) As R is an integral domain and $\det(S) \neq 0$ corollary (4.65.(ii)) tells us that $\mathrm{kn}(S) = 0$. That is for any $x \in R^m$ we have $Sx = 0$ if and only if $x = 0$. On the other hand the columns of SA clearly are Sc_j

$$SA \;=\; \begin{pmatrix} | & | & & | \\ Sc_1 & Sc_2 & \dots & Sc_n \\ | & | & & | \end{pmatrix}$$

Thus if we regard some subset $J \subseteq 1 \dots n$ and $x_j \in R$, where $j \in J$ then for $x = \sum_j x_j c_j \in R^m$ we find the equivalence of

$$\sum_{j\in J} x_j c_j \;=\; 0 \quad\Longleftrightarrow\quad \sum_{j\in J} x_j S c_j \;=\; S\left(\sum_{j\in J} x_j c_j\right) \;=\; 0$$

Therefore $\{\, c_j \mid j \in J \,\}$ is linearly independent if and only if the set $\{\, Sc_j \mid j \in J \,\}$ is linearly independent. And as the Sc_j are the columns of SA this in particular means, that

$$\text{c-rank}(SA) \;=\; \text{c-rank}(A)$$

Note that this has been proved for any matrices A and S. Thus given A and T consider $B := A^*$ and $S := T^*$ then $AT = B^*S^* = (SB)^*$ and therefore we find

$$\text{r-rank}(AT) \;=\; \text{c-rank}(SB) \;=\; \text{c-rank}(B) \;=\; \text{r-rank}(A)$$

So far this has been proved without using that both ranks are equal, due to (v). If we also use that $\text{c-rank}(A) = \text{r-rank}(A)$ for any matrix A then we can complete the proof to full effect

$$\text{c-rank}(SAT) \;=\; \text{c-rank}(AT) \;=\; \text{r-rank}(AT)$$

$$\begin{aligned} &= \text{r-rank}(A) = \text{c-rank}(A) \\ \text{r-rank}(SAT) &= \text{r-rank}(SA) = \text{c-rank}(SA) \\ &= \text{c-rank}(A) = \text{r-rank}(A) \end{aligned}$$

(vii) In this statement R is assumed to be a PID. In particular we have c-rank(A) = r-rank(A), as this is true in any integral domain and c-rank$(A) \leq \min\{ m, n \}$ according to (i). It remains to prove c-rank(A) = i-rank(A) = rank(im(A)). So let $c_j := \text{col}_j(A)$ be the j-th column of A again (where $j \in 1 \ldots n$) and pick up a subset $J \in 1 \ldots n$ such that $\#J$ is maximal with the property that $\{ c_j \mid j \in J \}$ is linearly independent. That is $r := \#J =$ c-rank(A) and if we consider any $i \in 1 \ldots n \setminus J$, then there are some non-trivial $u_{i,j}$ and $v_i \in R$ such that

$$\sum_{j \in J} u_{i,j} c_j + v_i c_i = 0$$

As the $\{ c_j \mid j \in J \}$ are linearly independent this relation has to encompass c_i such that $v_i \neq 0$. Now define v the product of the v_i, where i runs along $i \notin J$ and let

$$C := \text{Lh}\{ c_j \mid j \in J \} \leq_{\mathtt{m}} R^m$$

Then $\{ c_j \mid j \in J \}$ is a basis of C, but as R is a PID and R^m is finitely generated and free, (3.104) tells us, that im(A) also is finitely generated and free. Also it is clear, that $C \subseteq$ im(A), as im$(A) = \text{Lh}\{ c_1, \ldots, c_n \}$. Hence we may pick up a basis $\{ x_1, \ldots, x_s \}$ of im(A). Recall

$$v_i c_i = -\sum_{j \in J} u_{i,j} c_j \in \text{Lh}\{ c_j \mid j \in J \} = C$$

$$v := \prod_{i \notin J} v_i \implies v c_i = \widehat{v_i} v_i c_i \in C$$

for any $i \in 1 \ldots n \setminus J$. And for $j \in J$ we have $c_j \in C$ by construction, such that $v c_i \in C$ is true for any $i \in 1 \ldots n$. But the image of A is generated by the columns of A, that is im$(A) = \text{Lh}\{ c_1, \ldots, c_n \}$ and in particular any x_k is of the form

$$x_k = \sum_{j=1}^{n} h_{j,k} c_j \implies v x_k = \sum_{j=1}^{n} h_{j,k} v c_j \in C$$

That is $\{ v x_1, \ldots, v x_s \} \subseteq C$. But as $v \neq 0$ and im(A) is free in particular torsion-free the set $\{ v x_1, \ldots, v x_s \}$ is linearly independent again: Suppose we had a relation on this set

$$0 = \sum_{k=1}^{s} a_k v x_k = v \sum_{k=1}^{s} a_k x_k \implies 0 = \sum_{k=1}^{s} a_k x_k$$

then this would yield a relation on the set $\{ x_1, \ldots, x_s \}$ itself. But as this is a basis this implies $a_1 = \cdots = a_s = 0$ such that $\{ v x_1, \ldots, v x_s \}$ is linearly independent, too. That is C contains the linearly independent set $\{ v x_1, \ldots, v x_s \}$, although it is an r-dimensional module, by construction.

Hence (3.104.(i)) implies $s \leq r$ and this has been (using (i) in the end)

$$\text{i-rank}(A) \;=\; \dim(\text{im}(A)) \;=\; s \;\leq\; r \;=\; \text{c-rank}(A) \;\leq\; \text{i-rank}(A)$$

(viii) In this statement R is assumed to be a skew field. We will prove the equality $\text{r-rank}(A) = \dim(N)$ only, as the proof of $\text{c-rank}(A) = \dim(M)$ is completely analogous. So let $p := \text{r-rank}(A)$ and $I \subseteq 1 \ldots m$ be one of those sets for which $\#I = p$ and r_I is R-linearly independent. If $p = m$, then $\{ r_1, r_2, \ldots, r_m \}$ is a basis of N and hence $\dim(N) = m = p$ is clear. Otherwise, since I is of maximal size we find that for any $k \in 1 \ldots m$ with $k \notin I$ the set $\{ r_i \mid i \in I \} \cup \{ r_k \}$ *is* linearly dependent. That is there are some $a_i \in R$ (not-all zero) such that

$$\sum_{i \in I} a_i r_i + a_k r_k \;=\; 0$$

If $a_k = 0$ then r_I already would be linearly dependent, which it is not. Hence we have $a_k \neq 0$ and since R is a skew-field this implies

$$r_k \;=\; \sum_{i \in I} \big(-a_k^{-1} a_i \big) r_i \;\in\; \text{Lh}(r_I)$$

And as this is true for any $k \notin I$ we find $N \subseteq \text{Lh}(r_I) \subseteq N$. So r_I generates N but also is linearly independent, therefore a basis of N. Hence

$$\text{r-rank}(A) \;=\; \#I \;=\; \#r_I \;=\; \dim(N)$$

Finally we have $\text{i-rank}(A) = \text{rank}(\text{im}(A)) = \text{rank}(M) = \dim(M)$, since R is a skew-field. This has been explained in remark (3.100).

(ix) The implication (b) $\Longrightarrow$ (a) is true for a general commutative ring and easy to see: Suppose there are some $a_1, a_2, \ldots, a_m \in R$ such that

$$\sum_{i=1}^{m} a_i \, x_i \;=\; 0$$

By (b) there is some $\alpha \in \text{Asc}(m, n)$ such that $\{ P_\alpha(x_1), \ldots, P_\alpha(x_m) \}$ is linearly independent. But as the projection P_α is R-linear we find

$$0 \;=\; P_\alpha \left(\sum_{i=1}^{m} a_i \, x_i \right) \;=\; \sum_{i=1}^{m} a_i \, P_\alpha(x_i)$$

The linear independence of the $P_\alpha(x_i)$ implies $a_1 = a_2 = \cdots = a_m = 0$ and hence the x_i are linearly independent themselves. Conversely let us define the matrix

$$A \;=\; \begin{pmatrix} | & | & & | \\ x_1 & x_2 & \ldots & x_m \\ | & | & & | \end{pmatrix} \;\in\; \text{mat}_{n,m}(R)$$

By assumption (a) we have $\text{c-rank}(A) = m$, but if R is an integral domain, then by (vi) we also

have r-rank(A) = c-rank$(A) = m$. That is there is some $\alpha \in \mathrm{Asc}(m,n)$ such that $\mathrm{row}_{\alpha(1)}(A)$ to $\mathrm{row}_{\alpha(m)}(A)$ are linearly independent. Thereby it is clear that

$$A' := \begin{pmatrix} \text{---} & \mathrm{row}_{\alpha(1)}(A) & \text{---} \\ & \vdots & \\ \text{---} & \mathrm{row}_{\alpha(m)}(A) & \text{---} \end{pmatrix} = \begin{pmatrix} | & & | \\ P_\alpha(x_1) & \dots & P_\alpha(x_m) \\ | & & | \end{pmatrix}$$

But since c-rank(A') = r-rank$(A') = m$ again, we find, that the $P_\alpha(x_i)$ are linearly independent. And this is precisely the claim of (b).

□

Proof of (4.79):
We will first prove the equivalences of (a), (b) and (c): If (a), that is c-rank$(A) = q \leq r$ then there is some $I \subseteq 1 \dots n$ with $\#I = q$ such that $\{ c_j \mid j \in J \}$ is linearly independent but for any $k \in 1 \dots n \setminus J$ the set $\{ c_j \mid j \in J \} \cup \{ c_k \}$ *is* linearly dependent. That is there are some a_j and $b \in F$ such that

$$\sum_{j \in J} a_j c_j + b c_k \;=\; 0$$

If $b = 0$ then we would also have $a_j = 0$ for any $j \in J$, as $\{ c_j \mid j \in J \}$ is linearly independent. But as c_k is linearly dependent we may assume otherwise. Now, since F is a field, this means:

$$c_k \;=\; \sum_{j \in J} (-a_j b^{-1}) c_j \;\in\; \mathrm{Lh}_F\{ c_j \mid j \in J \}$$

Of course any c_j for some $j \in J$ is contained in the linear hull Lh$\{ c_j \mid j \in J \}$, as well. And this remains true if we expand I to size r by adding random elements of $1 \dots n$. So we have arrived at (b).
Now assume (b), for ease of notation we may assume $J = 1 \dots r$, then by assumption any c_k can be expressed as a linear combination of c_1 to c_r

$$c_k \;=\; \sum_{i=1}^{r} a_{i,k} c_i$$

Thus if we define the matrix $C \in \mathrm{mat}_{m,r}(F)$ to have the columns $\mathrm{col}_i(C) = c_i$ and the matrix $R \in \mathrm{mat}_{r,n}(F)$ then proposition (4.20) tells us, that truly $A = C\,R$. So we have deduced (c).
For the first part it remains to show that (c) implies (a). But this is easy to see, using (4.72.(ii)) and (4.72.(i)) as these yield

$$\text{c-rank}(A) \;=\; \text{c-rank}(C\,R) \;\leq\; \text{c-rank}(R) \;\leq\; \min\{ r, n \} \;\leq\; r$$

In the next part we will prove the equivalence of (e), (d) and (c): Starting with (e) we have c-rank(A^*) = r-rank$(A) \leq r$ and hence (b) holds true for the columns of A^*. But as the columns of A^* are just the rows of A we find statement (d). Likewise (d) implies the decomposition $A^* = R^*\,C^*$ for some matrices $R^* \in \mathrm{mat}_{n,r}(F)$ and $C^* \in \mathrm{mat}_{r,m}(F)$. But transposing this equation we find (c) $A = C\,R$. And (c) in turn implies (e) by virtue of (4.72.(ii)) and (4.72.(i)) again:

$$\text{r-rank}(A) \;=\; \text{r-rank}(C\,R) \;\leq\; \text{r-rank}(C) \;\leq\; \min\{ m, r \} \;\leq\; r$$

In the third and final step we need to argue, that c-rank(A) equals r, where r is the minimal number such that there are some $C \in \mathrm{mat}_{m,r}(F)$ and $R \in \mathrm{mat}_{r,n}(F)$ such that $A = C\,R$. By (a) this already implies c-rank$(A) \leq r$. Suppose c-rank$(A) < r$, then by (c) there would be a decomposition $A = C'\,R'$ of smaller size. But as r was assumed to be minimal, this cannot be and hence c-rank$(A) = r$. Precisely the same reasoning also yields r-rank$(A) = r$ and hence r-rank(A) = c-rank(A), as well. □
The proof of (4.83.(vii)) requires substantial effort. We hence chose to export a part of the argument here. Due to its technicak natrue we do not deem it worthy to be presented in the first part of the book, though.

(15.1) Proposition: (viz. 926)
Let $(R, +, \cdot)$ be a commutative ring and $A \in \mathrm{mat}_{m,n}(R)$ where $n \leq m$. For $\alpha \in \mathrm{Asc}(n,m)$ let us denote the submatrix $A_\alpha = A[\alpha \mid \mathbb{1}] \in \mathrm{mat}_n(R)$ of A. Then all the coefficients of the product $AA^*_\alpha \in \mathrm{mat}_n(R)$ are taken from

$$\mathrm{ent}_{i,j}(AA^*_\alpha) \;\in \bigcup_{m \in \mathrm{Minor}_n(A)} \{\, m, -m, 0 \,\} \;\subseteq\; \mathfrak{f}_n(A)$$

Proof of (15.1):
Let us denote $A = (a_{i,k})$ and $A^*_\alpha = (a^\#_{j,k})$ where $i \in 1 \ldots m$ and $j, k \in 1 \ldots n$. Then by definition of the matrix multiplication we have

$$\begin{aligned}
\mathrm{ent}_{i,k}(AA^*_\alpha) &= \sum_{j=1}^{n} a_{i,j}\, a^\#_{j,k} \\
&= \sum_{j=1}^{n} a_{i,j}\, (-1)^{j+k} \det\big(A\,[\alpha \mid \mathbb{1}]_{k,j}\big) \\
&= \sum_{j=1}^{n} (-1)^{j+k} a_{i,j} \det\big(A\,[\alpha \mid \mathbb{1}]_{k,j}\big)
\end{aligned}$$

By the Laplace expansion theorem (4.55.(v)) this is precisely the expansion of the matrix B along the i-th row, where B is gained from A_α by replacing the k-th row of A_α by the j-th row of A. That is

$$\mathrm{ent}_{i,k}(AA^*_\alpha) \;=\; \det \begin{pmatrix}
\text{—— } \mathrm{row}_{\alpha(1)}(A) \text{ ——} \\
\vdots \\
\text{—— } \mathrm{row}_{\alpha(k-1)}(A) \text{ ——} \\
\text{—— } \mathrm{row}_{j}(A) \text{ ——} \\
\text{—— } \mathrm{row}_{\alpha(k+1)}(A) \text{ ——} \\
\vdots \\
\text{—— } \mathrm{row}_{\alpha(n)}(A) \text{ ——}
\end{pmatrix}$$

If $j \in \{\, \alpha(1), \ldots, \alpha(k-1), \alpha(k+1), \ldots, \alpha(n) \,\}$ then $\mathrm{row}_j(A)$ appears twice in this matrix and hence the determinant is 0 in this case. If not we can permute the rows of this matrix such that the order of the rows matches the order of the rows of A. But as permuting the rows only changes the sign of the determinant, we find that $\mathrm{ent}_{i,k}(AA^*_\alpha) = \pm m$ for some $m \in \mathrm{Minor}_n(A)$. □

Proof of (4.83):

(i) As usual let A have the entries $A = (a_{i,j})$ and fix some $i \in 1 \ldots r$ and $j \in 1 \ldots s$. Then we take a

look at the (j,i)-th entry of the two matrixes in question:

$$\mathrm{ent}_{j,i}\,(A[\alpha \mid \beta]^*) \;=\; \mathrm{ent}_{i,j}\,(A[\alpha \mid \beta]) \;=\; a_{\alpha(i),\beta(j)}$$

$$\mathrm{ent}_{j,i}\,(A^*[\beta \mid \alpha]) \;=\; a^*_{\beta(j),\alpha(i)} \;=\; a_{\alpha(i),\beta(j)}$$

Here we can clearly see, that these entries agree and hence the matrices are equal as a whole. But as the determinant is invariant under transposition this implies

$$\det\,(A[\alpha \mid \beta]) \;=\; \det\,(A^*[\beta \mid \alpha])$$

Varying α and β over all ascending chains of indexes in $\mathrm{Asc}(r,m)$ and $\mathrm{Asc}(r,n)$ respectively we collect all the minors of A and A^*

$$\begin{aligned}\mathrm{Minor}_r(A) &= \{\,\det\,(A[\alpha \mid \beta]) \mid \alpha \in \mathrm{Asc}(r,m),\, \beta \in \mathrm{Asc}(r,n)\,\}\\ &= \{\,\det\,(A^*[\beta \mid \alpha]) \mid \alpha \in \mathrm{Asc}(r,m),\, \beta \in \mathrm{Asc}(r,n)\,\}\\ &= \mathrm{Minor}_r(A^*)\end{aligned}$$

In particular we have $\mathrm{Minor}_r(A) = \{0\}$ if and only if $\mathrm{Minor}_r(A^*) = \{0\}$. And as this have been used to define the minorial rank we have $\text{m-rank}(A) = \text{m-rank}(A^*)$. As the Fitting ideal $\mathfrak{f}_r(A)$ is generated by $\mathrm{Minor}_r(A)$ we also find $\mathfrak{f}_r(A) = \mathfrak{f}_r(A^*)$. But as the annihilators of these ideals have been used to define the Fitting rank, we clearly have $\text{f-rank}(A) = \text{f-rank}(A^*)$, as well.

(ii) The proof of this statement is a tedious distinction of several cases - it will be conducted in several steps - the first two steps are the technical part, the later parts will be applications of this, that will yield the claim by induction

- We will first prove that for any permutation matrix $P \in \mathrm{mat}_m R$

$$\pm\,\mathrm{Minor}_r(P\,A) \;\subseteq\; \pm\,\mathrm{Minor}_r(A)$$

Thus choose any $\alpha \in \mathrm{Asc}(r,m)$ and $\beta \in \mathrm{Asc}(r,n)$ and suppose $P = P(\sigma)$. Then define $\alpha' \in \mathrm{Asc}(r,m)$ to be the chain of indexes with scope $\alpha'(1\ldots r) = \sigma(\alpha(1\ldots r))$ and define $\sigma' \in S_r$ to be the permutation that satisfies $\alpha' \circ \sigma' = \sigma \circ \alpha$. Then it is clear that

$$P(\sigma)A\,[\alpha \mid \beta] \;=\; P(\sigma')\,A[\alpha' \mid \beta]$$

And hence the minor of PA selected by $[\alpha \mid \beta]$ is just the minor of A selected by $[\alpha' \mid \beta]$ (up to the sign of $P(\sigma')$).

- Now we will prove that for any transvection matrix $T \in \mathrm{mat}_m(R)$

$$\mathrm{Minor}_r(T\,A) \;\subseteq\; \mathrm{Minor}_r(A)$$

Thus choose any $\alpha \in \mathrm{Asc}(r,m)$ and $\gamma \in \mathrm{Asc}(r,n)$, then the Cauchy-Binet-formula reads as

$$\det(TA[\alpha \mid \gamma]) \;=\; \sum_{\beta \in \mathrm{Asc}(r,m)} \det(T[\alpha \mid \beta])\det(A[\beta \mid \gamma])$$

It is clear that the submatrix $T[\alpha \mid \beta]$ is a triangular matrix, since T was such. Thus the determinant only depends on the entries in the diagonal. In the case $\alpha = \beta$ all these diagonal entries are 1 and hence $\det(\mathrm{ent}_{\alpha,\alpha} T) = 1$. In the case $\alpha \neq \beta$ there is (at least one) 0 on the diagonal and hence $\det(T[\alpha \mid \beta]) = 0$. Thus the sum over β collapses to the case $\beta = \alpha$ and hence

$$\det(TA\,[\alpha \mid \gamma]) \;=\; \det(A[\alpha \mid \gamma])$$

In other words the respective minor just remains unchanged.

- In the previous two steps we have seen that for any elementary matrix $E \in \mathrm{mat}_m(R)$ we get

$$\pm\,\mathrm{Minor}_r(E\,A) \;\subseteq\; \pm\,\mathrm{Minor}_r(A)$$

But with E also E^{-1} is an elementary matrix and $A = E^{-1}\,E\,A$. Therefore we can use this inclusion twice to obtain

$$\pm\,\mathrm{Minor}_r(A) \;\subseteq\; \pm\,\mathrm{Minor}_r(E\,A) \;\subseteq\; \pm\,\mathrm{Minor}_r(A)$$

- Thus we have seen that for any elementary matrix $E \in \mathrm{mat}_m R$

$$\pm\,\mathrm{Minor}_r(E\,A) \;=\; \pm\,\mathrm{Minor}_r(A)$$

As the determinant is invariant under transposition of matrices we see that for any elementary matrix $F \in \mathrm{mat}_n R$ we also get

$$\pm\,\mathrm{Minor}_r(A\,F) \;=\; \pm\,\mathrm{Minor}_r(A)$$

- Thus if A and B are elementary equivalent by virtue of the matrices $E_1, \ldots, E_r \in \mathrm{mat}_m R$ and $F_1, \ldots, F_s \in \mathrm{mat}_n R$

$$A \;\equiv\; B \;=\; E_1 \ldots E_r\,A\,F_1 \ldots F_s$$

Then we may easily use induction on the number $r + s$ of elementary matrices taking the previous part as the induction step.

(iii) For $r = 1$ the statements are trivial, as $\mathfrak{f}_0(A) = R$ and $\mathfrak{f}_1(A) \subseteq \mathfrak{f}_1(A)^1$ is clear. Thus let us consider $r \geq 2$ only: If $m \in \mathrm{Minor}_r(A)$ is an r-minor of A, then $m = \det(A')$ for some $(r \times r)$-submatrix A' of A. But using Laplace expansion of A' along the first column we see that

$$m \;=\; \sum_{i=1}^{r} (-1)^{i+1} a'_{i,1} \det(A'_{i,1})$$

It is clear that $\det(A'_{i,1}) \in \mathrm{Minor}_{r-1}(A)$ is an $(r-1)$-minor of A. Thus if $\mathrm{Minor}_{r-1}(A) = \{0\}$ then all these $\det(A'_{i,1}) = 0$ are zero and hence $m = \det(A') = 0$, as well. Therefore we have

$$\mathrm{Minor}_{r-1}(A) \;=\; \{0\} \quad\Longrightarrow\quad \mathrm{Minor}_r(A) \;=\; \{0\}$$

Also we find $m \in \mathrm{Lh}(\mathrm{Minor}_{r-1}(A)) \;=\; \mathfrak{f}_{r-1}(A)$. But as m was any r-minor of A this means

$\mathrm{Minor}_r(A) \subseteq \mathfrak{f}_{r-1}(A)$ and hence even

$$\mathfrak{f}_r(A) \quad \subseteq \quad \mathfrak{f}_{r-1}(A)$$

In fact we find even more: Let us finally prove $\mathrm{Minor}_r(A) \subseteq \mathfrak{f}_1(A)^r$ by induction on r. The case $r = 1$ is trivial, so by induction hypothesis we already have $\mathrm{Minor}_{r-1}(A) \in \mathfrak{f}_1(A)^{r-1}$. Looking at m above we note, that $a'_{i,1} \in \mathfrak{f}_1(A)$ and $\det(A'_{i,1}) \in \mathrm{Minor}_{r-1}(A)$. By induction hypothesis this is $\det(A'_{i,1}) \subseteq \mathfrak{f}_1(A)^{r-1}$ such that

$$m \;\in\; \mathfrak{f}_1(A) \cdot \mathfrak{f}_1(A)^{r-1} \;=\; \mathfrak{f}_1(A)^r$$

As $m \in \mathrm{Minor}_r(A)$ has been an arbitrary minor of A, this of course implies $\mathrm{Minor}_r(A) \subseteq \mathfrak{f}_1(A)^r$ and hence $\mathfrak{f}_r(A) \subseteq \mathfrak{f}_1(A)^r$.

(iv) Since the fitting ideal $\mathfrak{f}_r(A)$ is generated by the set $\mathrm{Minor}_r(A)$ of r-minors of A we can cite proposition (3.22.(iv)) to see

$$\begin{aligned} \mathrm{ann}\,(\mathfrak{f}_r(A)) &= \mathrm{ann}\,(\mathrm{Minor}_r(A)) \\ &= \bigcap \{\, \mathrm{ann}(m) \mid m \in \mathrm{Minor}_r(A) \,\} \\ &= \{\, a \in R \mid \forall\, m \in \mathrm{Minor}_r(A) \,:\, am = 0 \,\} \end{aligned}$$

And as by (ii) we have $\mathfrak{f}_r(A) \subseteq \mathfrak{f}_{r-1}(A)$ then annihilators of these ideals clearly satisfy the converse inclusion

$$\mathrm{ann}\,(\mathfrak{f}_{r-1}(A)) \;\subseteq\; \mathrm{ann}\,(\mathfrak{f}_r(A))$$

(v) If $A' = A[\alpha \mid \beta]$ is a submatrix of A, then $\mathrm{Minor}_r(A') \subseteq \mathrm{Minor}_r(A)$ is obvious, for any $r \in \mathbb{N}$. If now $r = \text{m-rank}(A')$ then by definition there is some $m \in \mathrm{Minor}_r(A')$ such that $m \neq 0$. But then $0 \neq m \in \mathrm{Minor}_r(A)$, as well. And as the minorial rank of A has been defined to be the *maximal* number r with this property we have

$$\text{m-rank}(A') \;=\; r \;\leq\; \text{m-rank}(A)$$

Also $\mathrm{Minor}_r(A') \subseteq \mathrm{Minor}_r(A)$ implies $\mathfrak{f}_r(A') \subseteq \mathfrak{f}_r(A)$ and hence the annihilator ideals satisfy $\mathrm{ann}(\mathfrak{f}_r(A)) \subseteq \mathrm{ann}(\mathfrak{f}_r(A'))$ the opposite inclusion. If now $r = \text{f-rank}(A')$ then $\mathrm{ann}(\mathfrak{f}_r(A')) = 0$ and due to the inclusion $\mathrm{ann}(\mathfrak{f}_r(A)) = 0$. And as the Fitting rank of A has been defined to be the *maximal* number r with this property we have

$$\text{f-rank}(A') \;=\; r \;\leq\; \text{f-rank}(A)$$

(vi) Let us first assume $A \in \mathrm{mat}_r(R)$ is a square matrix with $\text{f-rank}(A) = r$. Then we have to show $\text{r-rank}(A) = \text{c-rank}(A) = r$. By assumption

$$0 \;=\; \mathrm{ann}(\mathfrak{f}_r(A)) \;=\; \mathrm{ann}(\det(A))$$

Let now $A_j := \mathrm{col}_j(A)$ be the j-th column of A and consider some $a_j \in R$ such that the following

linear relation holds true

$$\sum_{j=1}^{n} a_j A_j \;=\; 0$$

We will prove, that in this case we already have $a_1 = 0$. In complete analogy we could prove $a_j = 0$ for any $j \in 1 \ldots r$, but specialize to the case $j = 1$ for ease of notation. To do this simply compute

$$\begin{aligned} a_1 \det(A) &= a_1 \det(A_1, A_2, \ldots, A_n) \;=\; \det(a_1 A_1, A_2, \ldots, A_n) \\ &= \det\left(\sum_{j=2}^{n} -a_j A_j, A_2, \ldots, A_n\right) \\ &= \sum_{j=2}^{n} -a_j \det(A_j, A_2, \ldots, A_n) \end{aligned}$$

As any determinant in the last term contains A_j twice, it vanishes. That is we have $a_1 \det(A) = 0$, but as $\operatorname{ann}(\det(A)) = 0$ this implies $a_1 = 0$. That is the columns A_1 to A_n of A are linearly independent, c-rank$(A) = r$. And as this has been proved for any matrix A, we can apply it to A^*: By (i) we have f-rank(A^*) = f-rank$(A) = r$ and hence we find r-rank(A) = c-rank$(A^*) = r$, as well.

For the general statement let $A' := A[\alpha \mid \beta] \in \mathrm{mat}_r(R)$. By assumption we have $\operatorname{ann}(\det(A')) = 0$ such that by the above we find r-rank$(A') = r$ and c-rank$(A') = r$. But as the rank of the submatrix A' cannot exceed the rank of A - this is (4.72.(iii)) - we find c-rank$(A) \geq$ c-rank$(A') = r$ and r-rank$(A) \geq$ r-rank$(A') = r$.

(vii) Let $r :=$ m-rank(AB) and suppose $r >$ m-rank(A). This would mean $\det(A[\alpha \mid \beta]) = 0$ for any $\alpha \in \mathrm{Asc}(r,k)$ and any $\beta \in \mathrm{Asc}(r,m)$. Likewise if $r >$ m-rank(B) then $\det(B[\beta \mid \gamma]) = 0$ for any $\beta \in \mathrm{Asc}(r,m)$ and any $\gamma \in \mathrm{Asc}(r,n)$. Now take a look at the formula of Cauchy-Binet

$$\det\big(AB[\alpha \mid \gamma]\big) \;=\; \sum_{\beta \in \mathrm{Asc}(r,m)} \det\big(A[\alpha \mid \beta]\big) \det\big(B[\beta \mid \gamma]\big)$$

But by assumption $r =$ m-rank(AB) there are some α and γ such that $\det(AB[\alpha \mid \gamma]) \neq 0$. Thus neither all the $\det(A[\alpha \mid \beta])$ nor all the $\det(B[\beta \mid \gamma])$ may all be zero. In particular this means $r \leq$ m-rank(A) and $r \leq$ m-rank(B).

(viii) First of all we note, that all these statements are false in case $m < n$: By definition we have f-rank$(A) \leq m < n$ and c-rank$(A) \leq m < n$ is true by (4.72.(i)). In this case we also have $\mathrm{kn}(A) \neq 0$, since

$$R^n \;\cong_{\mathsf{m}}\; R^n \big/ \mathrm{kn}(A) \;\cong_{\mathsf{m}}\; \mathrm{im}(A) \;\subseteq\; R^m$$

Clearly R^n contains n linearly independent elements [namely $e_j \in R^n$ the Euclidean base vectors]. But as R^m is generated by $m < n$ elements [namely the Euclidean base vectors $e_i \in R^m$] any n elements of R^m are linearly dependent, according to (3.99.(i)). But this contradicts the injective homomorphism $R^n \hookrightarrow R^m$ above. Thus throughout this proof we may assume $n \leq m$.

Let us begin with $\mathrm{kn}(A) = 0 \iff$ c-rank$(A) = n$. Denote the column vectors of A by $A_j :=$

$\mathrm{col}_j(A)$ where $j \in 1 \ldots n$ and suppose there was some relation of the form

$$x_1 A_1 + x_2 A_2 + \cdots + x_n A_n \;=\; 0 \;\in\; R^m$$

Note that $Ax = A_1 x_1 + A_n x_n$ is precisely that sum. Thus if we have c-rank$(A) = n$, then the A_j are linearly independent, such that $Ax = 0$ implies $x = 0$, which is just a reformulation of $\mathrm{kn}(A) = 0$. And if c-rank$(A) < n$ then there is some $x \in R^n$ with $x \neq 0$ but $Ax = 0$ which in turn means $x \in \mathrm{kn}(A)$ such that is this case $\mathrm{kn}(A) \neq 0$.

The hard part is the implication $\mathrm{kn}(A) = 0 \implies$ f-rank$(A) = n$, which we will do now. To do this we will use induction on n: The case $n = 1$ is quite obvious: We need to show $\mathrm{ann}(\mathrm{Minor}_1(A)) = 0$. In this case A is a single column vector $A = (c_1\, c_2\, \ldots\, c_m)^*$ only and hence $\mathrm{Minor}_1(A) = \{\, c_1, \ldots, c_m \,\}$ If we had $a \in \mathrm{ann}(\mathrm{Minor}_1(A))$ for some $a \neq 0$ then $a(c_1, c_2, \ldots, c_m) = 0 \in R^m$. That is the column vector of A would be linearly dependent (itself) in contradiction to c-rank$(A) = 1$. Thus we conclude f-rank$(A) = 1$, as well.

The clever part is the induction step: Suppose we have the implication c-rank$(A') = n-1 \implies$ f-rank$(A') = n-1$ for any $A' \in \mathrm{mat}_{q,n-1}(R)$ with $n - 1 \leq q$. Then we need to show this property for $A \in \mathrm{mat}_{m,n}(R)$ with $n \leq m$. That is we need $\mathrm{ann}(\mathrm{Minor}_n(A)) = 0$. Again we assume the opposite - there was some $a \neq 0$ with $a \in \mathrm{ann}(\mathrm{Minor}_n(R))$. Then for any $\alpha \in \mathrm{Asc}(n, m)$ let us denote the submatrix

$$A_\alpha \;:=\; A[\alpha \mid \mathbb{1}] \;\in\; \mathrm{mat}_n(A)$$

By (15.1) we know that all the coefficients of $AA^\#_\alpha$ are either 0 or $\pm m$ for some n-minor $m \in \mathrm{Minor}_n(A)$ of A. In particular

$$A\big(aA^\#_\alpha\big) \;=\; aAA^\#_\alpha \;=\; 0 \;\in \mathrm{mat}_{m,n}(R)$$

That is $A\, a\, \mathrm{col}_j(A^\#_\alpha) = 0 \in R^m$ for any $j \in 1 \ldots n$. But by assumption $\mathrm{kn}(A) = 0$ this means $a\, \mathrm{col}_j(A^\#_\alpha) = 0 \in R^n$ and as this is true for any j we find the annihilation

$$\forall\, \alpha \in \mathrm{Asc}(n, m) \;:\; aA^\#_\alpha \;=\; 0 \;\in\; \mathrm{mat}_n(R)$$

But clearly the coefficients of $A^\#_\alpha$ are $(n-1)$-minors of A and as α runs along all ascending chains of indices we have

$$\mathrm{Minor}_{n-1}(A) \;=\; \left\{\, a^\#_{\alpha(i),j} \mid \alpha \in \mathrm{Asc}(n, m),\, i, j \in 1 \ldots n \,\right\}$$

Since a annihilates all these coefficients we have $a \in \mathrm{ann}(\mathrm{Minor}_{n-1}(A))$ already. But if we look at the matrix

$$A' \;:=\; \begin{pmatrix} | & | & & | \\ \mathrm{col}_1(A) & \mathrm{col}_2(A) & \ldots & \mathrm{col}_{n-1}(A) \\ | & | & & | \end{pmatrix} \;\in\; \mathrm{mat}_{m,n-1}(R)$$

we have c-rank$(A') = n - 1$ and hence $\mathrm{kn}(A') = 0$ such that by induction hypothesis we have f-rank$(A') = n - 1$ [and $n - 1 \leq n \leq m$] again. That is $\mathrm{ann}(\mathrm{Minor}_{n-1}(A')) = 0$, but as the minors

of A' trivially are minors of A [that is $\mathrm{Minor}_{n-1}(A') \subseteq \mathrm{Minor}_{n-1}(A)$] we have

$$0 \neq a \;\in\; \mathrm{ann}(\mathrm{Minor}_{n-1}(A)) \;\subseteq\; \mathrm{ann}(\mathrm{Minor}_{n-1}(A')) \;=\; 0$$

That is we have arrived at a contradiction, which means there is no $a \neq 0$ with $a \in \mathrm{ann}(\mathrm{Minor}_n(A))$ such that $\text{f-rank}(A) = n$. So at long last we have arrived at the implication

$$\text{c-rank}(A) \;=\; n \quad\Longrightarrow\quad \text{f-rank}(A) \;=\; n$$

We finally have to show $\text{f-rank}(A) = n \implies \mathrm{kn}(A) = 0$ to complete the equivalence. This proof is easy again: As before let us denote $A_\alpha := A[\alpha \mid \mathbb{1}]$ again, for any $\alpha \in \mathrm{Asc}(n,m)$. Suppose we had some $x \in R^n$ with $x \neq 0$ and $Ax = 0$. As any A_α has the same rows as A (only a subset of these) this also means $A_\alpha x = 0$. But then

$$\det(A_\alpha)\, x \;=\; A_\alpha^\# A_\alpha\, x \;=\; A_\alpha^\# 0 \;=\; 0 \;\in\; R^n$$

Since there is some $k \in 1\ldots n$ with $x_k \neq 0$ this means $x_k \det(A_\alpha) = 0$. But as this is true for any $\alpha \in \mathrm{Asc}(n,m)$ we have $x_k m = 0$ for any $m \in \mathrm{Minor}_n(A)$ and hence $x_k \in \mathrm{ann}(\mathrm{Minor}_n(A))$. In particular we would have $\text{f-rank}(A) < n$ in contradiction to the assumption. And this means $Ax = 0 \implies x = 0$ such that $\mathrm{kn}(A) = 0$.

□

Proof of (4.86):
The theorem has three separate parts: The better the base ring R is, the more equalities we get for the rank of a matrix. We start with an arbitrary **commutative ring** $R \neq 0$. The first, easy step is to prove that generally $\text{f-rank}(A) \leq \text{m-rank}(A)$. But if $\mathrm{Minor}_r(A) = \{0\}$ then (as all $a \in R$ satisfy $a \cdot 0 = 0$) clearly $\mathrm{ann}(\mathfrak{f}_r(A)) = R \neq 0$. By negation this is the implication

$$\mathrm{ann}(\mathfrak{f}_r(A)) = 0 \quad\Longrightarrow\quad \mathrm{Minor}_r(A) \neq \{0\}$$

Thus if $r = \text{f-rank}(A)$ then this means $\mathrm{ann}(\mathfrak{f}_r(A)) = 0$ such that $\mathrm{Minor}_r(A) \neq \{0\}$. But as $\text{m-rank}(A)$ was defined to be the maximal number r with $\mathrm{Minor}_r(A) \neq \{0\}$ we find $\text{f-rank}(A) \leq \text{m-rank}(A)$.

In the next part we need to prove $\text{c-rank}(A) \leq \text{f-rank}(A)$. Likewise take $\text{c-rank}(A) = r$ then there is some $\beta \in \mathrm{Asc}(r,n)$ such that the submatrix $A' := A[\mathbb{1} \mid \beta] \in \mathrm{mat}_{m,r}(R)$ has full rank $\text{c-rank}(A') = r$. But then we find $\text{f-rank}(A') = r$ according to (4.83.(vii)) and hence

$$\text{f-rank}(A) \;\geq\; \text{f-rank}(A') \;=\; r \;=\; \text{c-rank}(A)$$

by (4.83.(iv)). Note that thereby the requirement $r \leq m$ is always satisfied since $r = \text{c-rank}(A) \leq m$ according to (4.72.(i)). Thus we have proved $\text{c-rank}(A) \leq \text{f-rank}(A)$ for a general matrix A. Once this is done it is clear that the row-rank of A also is bound, since $\text{r-rank}(A) = \text{c-rank}(A^*) \leq \text{f-rank}(A^*) = \text{f-rank}(A)$, where we used (4.83.(i)).

For an **integral domain** R we have already seen $\text{c-rank}(A) = \text{r-rank}(A)$ in (4.72.(vi)) and the equality $\text{f-rank}(A) = \text{m-rank}(A)$ is easy to see: In an integral domain $\mathrm{Minor}_r(A) = \{0\}$ even is equivalent to

$\operatorname{ann}(\mathfrak{f}_r(A)) \neq 0$. By negation this is the equivalence of

$$\operatorname{Minor}_r(A) \neq \{0\} \iff \operatorname{ann}(\mathfrak{f}_r(A)) = 0$$

As the Fitting and the minorial rank of A have been defined to be the maximal number r with the respective property they have to be equal

$$\text{m-rank}(A) \;=\; \text{f-rank}(A)$$

So it suffices to show $\text{c-rank}(A) = \text{m-rank}(A)$, which we will do now: If $r = \text{m-rank}(A)$, then there are some $\alpha \in \operatorname{Asc}(r,m)$ and $\beta \in \operatorname{Asc}(r,n)$ with

$$\det\big(A[\alpha \mid \beta]\big) \;\neq\; 0$$

Let us define the projection $P_\alpha : R^m \to R^r$ by $P_\alpha(a) := a'$ where for $a = (a_1,\ldots,a_m)$ we let $a' := (a_{\alpha(1)},\ldots,a_{\alpha(r)})$. If we also abbreviate the columns of A by $c_j := \operatorname{col}_j(A)$ for any $j \in 1\ldots n$ then clearly

$$A[\alpha \mid \beta] \;=\; \begin{pmatrix} | & & | \\ P_\alpha(c_{\beta(1)}) & \ldots & P_\alpha(c_{\beta(r)}) \\ | & & | \end{pmatrix}$$

Since the determinant of this matrix is non-zero corollary (4.65.(ii)) tells us, that the $P_\alpha(c_{\beta(i)})$ are linearly independent. Now suppose there was an R-linear combination $a_1 c_{\beta(1)} + \cdots + a_r c_{\beta(r)} = 0$ in R^m, then

$$0 \;=\; P_\alpha\left(\sum_{i=1}^{r} a_i c_{\beta(i)}\right) \;=\; \sum_{i=1}^{r} a_i P_\alpha\left(c_{\beta(i)}\right)$$

But since these are R-linearly independent we have $a_i = 0$ for all $i \in 1\ldots r$ and this means the $c_{\beta(i)}$ themselves are R-linearly independent. In particular A has r many linearly independent rows and hence

$$\text{m-rank}(A) \;= r \;\leq\; \text{c-rank}(A)$$

Conversely let $r := \text{c-rank}(A)$, then there is some $\beta \in \operatorname{Asc}(r,n)$ such that the columns $\left\{ c_{\beta(1)},\ldots,c_{\beta(r)} \right\} \subseteq R^m$ are R-linearly independent. That is the submatrix A' of A

$$A' \;:=\; A[\mathbb{1} \mid \beta] \;=\; \begin{pmatrix} | & & | \\ c_{\beta(1)} & \ldots & c_{\beta(r)} \\ | & & | \end{pmatrix}$$

has $\text{c-rank}(A') = r$. But as $\text{r-rank}(A') = \text{c-rank}(A') = r$ this means, that there also is some $\alpha \in \operatorname{Asc}(r,m)$ such that $\left\{ \operatorname{row}_{\alpha(i)}(A') \mid i \in 1\ldots r \right\}$ is R-linearly independent. But this is

$$A[\alpha \mid \beta] \;=\; \begin{pmatrix} \text{---} & \operatorname{row}_{\alpha(1)}(A') & \text{---} \\ & \vdots & \\ \text{---} & \operatorname{row}_{\alpha(r)}(A') & \text{---} \end{pmatrix}$$

As the rows of $A[\alpha \mid \beta]$ are linearly independent corollary (4.65.(ii)) again intervenes to provide $\det(A[\alpha \mid \beta]) \neq 0$. That is we have found an $(r \times r)$-minor of A that is non-zero and hence

$$\text{c-rank}(A) \;\; = r \;\; \leq \;\; \text{m-rank}(A)$$

Finally, in case R even is a **field**, it is both an integral domain and a skew field. But (4.72.(vii)) tells us, that in a skew field the image-rank then equals the column rank $\text{i-rank}(A) = \text{c-rank}(A)$ and all the other equalities have already been shown in case of an integral domain. □

Proof of (4.88):
The proof of (i) is a non-algorithmical trick computation. However it is far from being trivial and hence presented here. Then (ii) is clear, simply apply (i) to the transpose matrix A^* of A.

(ii) We begin by proving the existence of such a representation of A by a divisibly ascending chain of scalar factors. This will be the major part of the proof, the representation of the scalar factors in terms of minors then is simple

- First of all we define - for any matrix $0 \neq A = (a_{i,j}) \in \text{mat}_{m\times n}R$

$$\nu(A) \;\; := \;\; \min\{\, \nu(a_{i,j}) \mid i \in 1 \ldots m,\, j \in 1 \ldots n,\, a_{i,j} \neq 0 \,\}$$

 Now we regard the set of all $\nu(B)$ where B is a matrix that is elementarily equivalent to A

$$\{\, \nu(B) \mid B \in \text{mat}_{m\times n}R,\, A \equiv B \,\} \;\; \subseteq \;\; \mathbb{N}$$

 As $\mathbb{N}$ is well-ordered this set has a minimum and we choose such a matrix M for which $\nu(M)$ is minimal.

- Suppose that the (i,j)-th entry $m_{i,j}$ of M takes the minimal value $\nu(M) = \nu(m_{i,j})$. Then we may rearrange M to shift $m_{i,j}$ to the position $(1,1)$ and we denote this rearranged matrix by

$$M' \;\; := \;\; P(1\,i)\, M\, P(1\,j)$$

 I.e. $\text{ent}_{1,1}M' = \text{ent}_{i,j}M = m_{i,j}$ and hence $\nu(M') = \nu(\text{ent}_{1,1}M')$. Thus we may equally well assume that $\nu(M) = \nu(m_{1,1})$

- We now claim that $m_{1,1}$ divides all the entries $m_{i,1}$ in the first column of M. To see this we use division with remainder

$$m_{i,1} \;\; = \;\; p_i m_{1,1} + r_i \quad \text{where} \quad 0 \;\leq\; \nu(r_i) \;<\; \nu(m_{1,1})$$

 Suppose $r_i \neq 0$ then we would obtain a matrix $B := T_{i,1}(-p_i)\, M$ being elementary equivalent to M and hence to A, too. Clearly the $(i,1)$-entry of B is given to be

$$[\text{row}_i B]_1 \;\; = \;\; [\text{row}_i M - p_i \text{row}_1 M]_1 \;\; = \;\; m_{i,1} - p_i m_{1,1} \;\; = \;\; r_i$$

 Therefore $\nu(B) \leq \nu(r_i) < \nu(m_{1,1}) = \nu(M)$, but M was chosen to be minimal, so this cannot occur.

- Analogously we see that $m_{1,1}$ divides all the entries $m_{1,j}$ in the first row of M. We use division with remainder again

$$m_{1,j} \;=\; q_j m_{1,1} + s_i \quad \text{where} \quad 0 \;\leq\; \nu(s_j) \;<\; \nu(m_{1,1})$$

Suppose $s_j \neq 0$ then we would obtain a matrix $B := M\,T_{1,j}(-q_j)$ that is elementary equivalent to A again. Clearly the $(1,j)$-entry of B is then given to be

$$\big[\mathrm{col}_j B\big]_1 \;=\; \big[\mathrm{col}_j M - q_j \mathrm{col}_1 M\big]_1 \;=\; m_{1,j} - q_j m_{1,1} \;=\; s_j$$

Therefore $\nu(B) \leq \nu(s_j) < \nu(m_{1,1}) = \nu(M)$, but M was chosen to be minimal, so this cannot occur.

- We now use elementary transpositions to replace the entries of the first column $m_{i,1} \mapsto r_i = 0$ and of the first row $m_{1,j} \mapsto s_j = 0$. And this obviously is accomplished by

$$N \;:=\; T_{2,1}(-p_2)\ldots T_{m,1}(-p_m)\,M\,T_{1,2}(-q_2)\ldots T_{1,n}(-q_n)$$

As we have seen this matrix N now is of the following form

$$N \;=\; \begin{pmatrix} m_{1,1} & 0 & \ldots & 0 \\ 0 & * & \ldots & * \\ \vdots & \vdots & & \vdots \\ 0 & * & \ldots & * \end{pmatrix}$$

Let us abbreviate $N = S\,M\,T$ where S and T denote the respective products of transposition matrices. Then we will have a look at the entries of N for

$$\begin{aligned} \mathrm{ent}_{i,j} N &= [\mathrm{col}_j S\,M\,T]_i \\ &= [\mathrm{col}_j S\,M - q_j \mathrm{col}_1 S\,M]_i \\ &= \mathrm{ent}_{i,j} S\,M - q_j \mathrm{ent}_{i,1} S\,M \\ &= m_{i,j} - p_i m_{1,j} \\ &= m_{i,j} - p_i q_j m_{1,1} \end{aligned}$$

- We finally prove that $m_{1,1} = n_{1,1}$ even divides any other entry $n_{i,j} = m_{i,j} - p_i q_j m_{1,1}$ (with $i \in 2\ldots m$ and $j \in 2\ldots n$) of N as well. First we use division with remainder once more

$$n_{i,j} \;=\; h_{i,j} n_{1,1} + k_{i,j} \quad \text{where} \quad 0 \;\leq\; \nu(k_{i,j}) \;<\; \nu(n_{1,1})$$

Now regard the matrix $N' := T_{i,1}(1)\,N$, clearly the i-th row of N' assumes the form

$$\mathrm{row}_i N' \;=\; \mathrm{row}_i N + \mathrm{row}_1 N \;=\; \begin{pmatrix} n_{1,1} & n_{i,2} & \ldots & n_{i,n} \end{pmatrix}$$

Thus defining $N'' := N'\,T_{1,j}(-h_{i,j})$ yields another matrix with

$$\mathrm{col}_j N'' \;=\; \mathrm{col}_j N' - h_{i,j}\mathrm{col}_1 N' \;=\; \begin{pmatrix} \vdots \\ k_{i,j} \\ \vdots \end{pmatrix}$$

Hence $\nu(N'') \leq \nu(k_{i,j}) < \nu(n_{1,1}) = \nu(M)$. But N'' is elementarily equivalent to N and hence to A and as M was chosen to minimal among these matrices we find $k_{i,j} = 0$ again.

- Thus we have decomposed N into a scalar block $(m_{1,1})$ and a scalar multiple of a block A_1 of the size $(m-1)\times(n-1)$

$$N \;=\; (m_{1,1}) \oplus (m_{1,1}\,A_1)$$

Thus we let $d_1 := m_{1,1}$ and recurse the entire process starting with A_1. Using induction we find after $m-1$ steps that A truly is equivalent to a matrix D of the claimed form.

- Until now we have shown that A is elementarily equivalent to D

$$A \;\equiv\; D \;=\; \begin{pmatrix} d_1 & & 0 & 0 & \dots & 0 \\ & \ddots & & \vdots & & \vdots \\ 0 & & d_m & 0 & \dots & 0 \end{pmatrix}$$

As the determinant of a submatrix of D always is a product of the coefficients of the submatrix (and hence of D) we find

$$\{0\} \cup \left\{ d_{\alpha(1)} \dots d_{\alpha(r)} \mid \alpha \in A(r,m) \right\} \;=\; \mathrm{Minor}_r D$$

Since the d_i form a divisibly ascending chain it is clear that the greatest common divisor of these elements is just $d_1 \dots d_r$. But by (ii) the gcd of the minors is invariant under elementary equivalence and therefore

$$d_1 \dots d_r \;\in\; \gcd(\mathrm{Minor}_r D) \;=\; \gcd(\mathrm{Minor}_r A)$$

□

Proof of (4.93):
The only thing we need to check here are the additional properties (4) and (5) of a sesqui-linear form s. But this is straightforward: Let $x, y, z \in M$ and $a \in R$, then we may compute

$$\begin{aligned} s(x \mid y+z) &= \varepsilon\big(s(y+z \mid x)\big) \;=\; \varepsilon\big(s(y \mid x) + s(z \mid x)\big) \\ &= \varepsilon\big(s(y \mid x)\big) + \varepsilon\big(s(z \mid x)\big) \;=\; s(x \mid y) + s(x \mid z) \\ s(x \mid ay) &= \varepsilon\big(s(ay \mid x)\big) \;=\; \varepsilon\big(as(y \mid x)\big) \\ &= \varepsilon(a) \cdot \varepsilon\big(s(y \mid x)\big) \;=\; \varepsilon(a) \cdot s(x \mid y) \end{aligned}$$

□

Proof of (4.92):
Consider $t = (t_1, \ldots, t_n)$, $w = (w_1, \ldots, w_n)$ and $z = (z_1, \ldots, z_n) \in \mathbb{C}^n$ where $t_k = r_k + is_k$, $w_k = u_k + iv_k$ and $z_k = x_k + iy_k$ respectively. Then the first few identities are straightforward computations:

$$\begin{aligned}
\langle t + w \mid z\rangle &= \sum_{k=1}^{n} (t_k + w_k)\overline{z}_k \;=\; \sum_{k=1}^{n} t_k\overline{z}_k + \sum_{k=1}^{n} w_k\overline{z}_k \\
&= \langle t \mid z\rangle + \langle w \mid z\rangle \\
\langle aw \mid z\rangle &= \sum_{k=1}^{n} (aw_k)\overline{z}_k \;=\; a\sum_{k=1}^{n} w_k\overline{z}_k \\
&= a\langle w \mid z\rangle \\
\langle z \mid w\rangle &= \sum_{k=1}^{n} z_k\overline{w}_k \;=\; \sum_{k=1}^{n} \overline{z}_k\overline{w}_k \;=\; \overline{\sum_{k=1}^{n} \overline{z}_k w_k} \\
&= \overline{\langle w \mid z\rangle}
\end{aligned}$$

That is we have verified the three properties of a sesqui-linear form with respect to the complex conjugation and hence we already get the other properties, by (4.93). Next we have $w_k\overline{z}_k = (u_k + iv_k)(x_k - iy_k) = (u_k x_k + v_k y_k) + i(u_k y_k - v_k x_k)$. And from this we get

$$\begin{aligned}
\langle w \mid z\rangle &= \sum_{k=1}^{n} w_k\overline{z}_k \\
&= \sum_{k=1}^{n} \big((u_k x_k + v_k y_k) + i(u_k y_k - v_k x_k)\big) \\
&= \langle u, x\rangle + \langle v, y\rangle + i\big(\langle u, y\rangle - \langle v, x\rangle\big)
\end{aligned}$$

Here we can evaluate the real and imaginary part of $\langle w \mid z\rangle$ to find the formulas we have given in the proposition. By the construction of the inner product we have

$$\langle z \mid z\rangle \;=\; \sum_{k=1}^{n} z_k\overline{z}_k \;=\; \sum_{k=1}^{n} |z_k|^2$$

Thus if we take $|z| := (|z_1|, \ldots, |z_n|) \in \mathbb{R}^n$ we see that $\langle z \mid z\rangle = \langle |z|, |z|\rangle$. But as the scalar product on $\mathbb{R}^n$ is positive definite we see that $\langle z \mid z\rangle \geq 0$ is positive and if $\langle z \mid z\rangle = 0$ then we get $|z_k| = 0$ and hence $z_k = 0$ for any $k \in 1 \ldots n$. Hence $\langle z \mid z\rangle = 0$ implies $z = 0$, which means that the inner product even is positive definite. It remains to regard $w \in \mathbb{C}^n$, $z \in \mathbb{C}^m$ and $A \in \mathrm{mat}_{m,n}(\mathbb{C})$, then we compute

$$\begin{aligned}
\langle A\,w \mid z\rangle &= \sum_{r=1}^{m} \left(\sum_{s=1}^{n} a_{r,s} w_s\right) \overline{z}_r \\
&= \sum_{s=1}^{n} w_s \left(\sum_{r=1}^{m} a_{r,s}\overline{z}_r\right) \\
&= \sum_{s=1}^{n} w_s \overline{\sum_{r=1}^{m} \overline{a}_{r,s} z_r} \\
&= \sum_{s=1}^{n} w_s \overline{\sum_{r=1}^{m} \mathrm{ent}_{s,r}(\overline{A}) z_r} \\
&= \langle w \mid \overline{A}\,z\rangle
\end{aligned}$$

□

Proof of (4.97):

(i) Consider a linear relation of the g_i, that is for some $a_i \in R$ we have

$$\sum_{i\in I} a_i m_i \;=\; 0$$

Then for any $j \in J$ we could apply the linear map $x \mapsto s(x \mid m_j)$ to find $a_j = 0$ and thereby the linear independence of the m_i

$$0 = s(0 \mid m_j) = s\left(\sum_{i\in I} a_i m_i \mid m_j\right) = \sum_{i\in I} a_i s(m_i \mid m_j) = \sum_{i\in I} a_i \delta_{i,j} = a_j$$

(ii) As $\{ m_i \mid i \in I \}$ is a basis of M for any $x \in M$ there are uniquely determined coefficients $x_i \in R$ such that x can be written as

$$x \;=\; \sum_{i\in I} x_i m_i$$

For any $j \in I$ now apply $x \mapsto s(x \mid m_j)$ to this equation. Then we find that the coefficient x_j is given to be $x_j = s(x \mid m_j)$

$$s(x \mid m_j) = s\left(\sum_{i\in I} x_i m_i \mid m_j\right) = \sum_{i\in I} x_i s(m_i \mid m_j) = \sum_{i\in I} x_i \delta_{i,j} = x_j$$

(iii) In case of $R = \mathbb{R}$ or $R = \mathbb{C}$ the function r is easy to see: For $x \in M$ just take the positive square root $r(x) := \sqrt{\langle x \mid x\rangle} = \| x \|$. But let us check that it is possible to construct r in the general setting:

Since s is positive definite we have $s(x \mid x) \in Q$ for any $x \in M$ with $x \neq 0$ where $Q := \{ a \cdot \varepsilon(a) \mid a \in R^* \}$. So take a look at the map $\nu : R^* \twoheadrightarrow Q : a \mapsto a \cdot \varepsilon(a)$. We obtain an equivalence relation on R^* by letting $a \sim b$ if and only if $\nu(a) = \nu(b)$. The equivalence classes under this relation are the fibers $[b] = q^{-1}(\{ b \cdot \varepsilon(b) \})$. By the axiom of choice there is a subset $P \subseteq R^*$ such that $\overline{\nu} : P \longleftrightarrow Q : a \mapsto a \cdot \varepsilon(a)$. Now take $r(x) := \overline{\nu}^{-1}(s(x \mid x))$. Then r is a well-defined function r that satisfies $r(x) \in P \subseteq R^*$ and $r(x) \cdot \varepsilon(r(x)) = \overline{\nu}(r(x)) = s(x \mid x)$.

Now that we have defined $r : Q \to R^*$ we also have $N(x) = r(x)^{-1}x$ for $x \neq 0$. Note that $\mathrm{Lh}\{ x \} = \mathrm{Lh}\{ N(x) \}$ since $r(x)$ is a unit of R.

We will now prove that the Gram-Schmidt-Orthogonalisation Process truly yields an ONB of M with respect to s. We will use induction on k to verify the following properties

(1) g_k is well-defined

(1) $\{ g_1, \ldots, g_k \}$ is an ortho-normal system

(3) $\mathrm{Lh}\{ g_1, \ldots, g_k \} = \mathrm{Lh}\{ m_1, \ldots, m_k \}$

Starting with $k = 1$ we have $g_1 = N(m_1)$. And as $\{ m_1, \ldots, m_n \}$ is a basis [in particular linearly independent] we have $m_1 \neq 0$. Thus g_1 is well-defined, $\mathrm{Lh}\{ g_1 \} = \mathrm{Lh}\{ m_1 \}$ and we have

$$s(g_1 \mid g_1) \;=\; s\big(r(m_1)^{-1}m_1 \mid r(m_1)^{-1}m_1\big)$$

$$\begin{aligned} &= r(m_1)^{-1} \cdot \varepsilon(r(m_1)^{-1}) s(m_1 \mid m_1) \\ &= \big(r(m_1) \cdot \varepsilon(r(m_1))\big)^{-1} s(m_1 \mid m_1) \;=\; 1 \end{aligned}$$

For the induction step we may suppose the above statements (1), (2) and (3) for $\{ g_1, \ldots, g_{k-1} \}$. As $x \mapsto s(x \mid g_i)$ is linear, so is

$$P \;:\; M \to M \;:\; x \mapsto \sum_{i=1}^{k-1} s(x \mid g_i) g_i$$

And by induction hypothesis we have $\mathrm{im}(P) = \mathrm{Lh}\{ m_1, \ldots, m_{k-1} \}$. And as $\{ m_1, \ldots, m_n \}$ is a basis we therefore have $m_k \notin \mathrm{im}(P)$. In particular $q_k := m_k - P(m_k) \neq 0$ such that $a_k := r(q_k)$ and thereby $g_k = N(q_k) = a_k^{-1} q_k$ are well defined. Thereby $g_k \in \mathrm{im}(P) + Rm_k$ and conversely $m_k = P(m_k) + q_k \in \mathrm{im}(P) + Rg_k$ such that we also have property (3). It remains to prove (2): By induction hypothesis we already know $s(g_i \mid g_j) = \delta_{i,j}$ for any $i, j \in 1 \ldots k-1$. Now for any $j < k$ we compute

$$\begin{aligned} s(g_k \mid g_j) &= s\left(a_k^{-1} \big(m_k - P(m_k)\big) \mid g_j \right) \\ &= a_k^{-1} \big(s(m_k \mid g_j) - s(P(m_k) \mid g_j) \big) \\ &= a_k^{-1} \left(s(m_k \mid g_j) - \sum_{i=1}^{k-1} s(m_k \mid g_i)\, s(g_i \mid g_j) \right) \\ &= a_k^{-1} \left(s(m_k \mid g_j) - \sum_{i=1}^{k-1} s(m_k \mid g_i)\, \delta_{i,j} \right) \\ &= a_k^{-1} \big(s(m_k \mid g_j) - s(m_k \mid g_j) \big) \;=\; 0 \end{aligned}$$

Note that with $g(g_k \mid g_j) = 0$ we also have $s(g_j \mid g_k) = 0$ as s is symmetric up to ε and this is a homomorphism of rings. For $j = k$:

$$\begin{aligned} s(g_k \mid g_k) &= s\big(a_k^{-1} q_k \mid a_k^{-1} q_k\big) \\ &= a_k^{-1}\, \varepsilon\big(a_k^{-1}\big) s\big(q_k \mid q_k\big) \\ &= \big(a_k\, \varepsilon(a_k)\big)^{-1} s\big(q_k \mid q_k\big) \;=\; 1 \end{aligned}$$

The latter, as $a_k = r(q_k)$ and $r(q_k)\varepsilon(r(q_k)) = s(q_k \mid q_k)$ such that the inverse of $a_k \varepsilon(a_k)$ cancels $s(q_k \mid q_k)$. Altogether the induction is complete and thereby $\{ g_1, \ldots, g_n \}$ is an ortho-normal system again, that generates M. By (i) we know that any ortho-normal system is linear independent and hence $\{ g_1, \ldots, g_n \}$ is a basis of M.

□

Proof of (4.98):
It is clear that $U^\perp$ is a subspace of V as it is the intersection of the kernels of $x \mapsto s(x \mid u)$ which are subspaces of V. Also it is easy to see that $U \cap U^\perp = 0$. Suppose $u \in U \cap U^\perp$ then u lies in the kernel of $x \mapsto s(x \mid u)$ and hence $s(u \mid u) = 0$ Suppose we had $u \neq 0$, then $0 = s(u \mid u) \in \{ a\varepsilon(a) \mid a \in F^* \} \subseteq F^* = F \setminus \{0\}$. By that contradiction we have $u = 0$.
Next we prove $V = U + U^\perp$. To do this choose a basis $\{ v_1, \ldots, v_r \}$ of U and append it to a basis

$\{ v_1, \ldots, v_r, \ldots, v_n \}$ of V. Using the Gram-Schmidt-algorithm (4.97.(ii)) we can turn this basis into an ONB $\{ g_1, \ldots, g_r, \ldots, g_n \}$ of V with respect to ε. Let

$$\begin{aligned} U &= \mathrm{Lh}\{ v_1, \ldots, v_r \} = \mathrm{Lh}\{ g_1, \ldots, g_r \} \\ U' &:= \mathrm{Lh}\{ g_{r+1}, \ldots, g_n \} \end{aligned}$$

We will now prove that $U' \subseteq U^\perp$: For any $j \in (r+1) \ldots n$ and any $i \in 1 \ldots r$ we have $s(g_j \mid g_i) = 0$. As the g_i generate U this implies $s(g_j \mid u) = 0$ for any $u \in U$ and any $j \in (r+1) \ldots n$. But as the g_j generate U' we have $U' \subseteq U^\perp$.
But it is also clear, that $V = U + U'$, if we consider any $x \in V$, then [as $\{ g_1, \ldots, g_n \}$ is a basis of V] there are coefficients $x_k \in F$ such that x can be written in the form

$$x = \sum_{k=1}^{n} x_k v_k = \sum_{i=1}^{r} x_i v_i + \sum_{j=r+1}^{n} x_j v_j \in U + U'$$

Thus we have $V = U + U' \subseteq U + U^\perp \subseteq V$ and hence $V = U + U^\perp$. But we have already proved $U \cap U^\perp = 0$ such that $V = U \oplus U^\perp$ is the inner direct sum. Applying this argument to $U^\perp$ we find $V = U^\perp \oplus (U^\perp)^\perp$. But as $U^\perp = \mathrm{Lh}\{ g_{r+1}, \ldots, g_n \}$ it follows that $(U^\perp)^\perp = \mathrm{Lh}\{ g_1, \ldots, u_r \} = U$.
Let us finish the proof by showing $U' = U^\perp$: We have already seen $U' \subseteq U^\perp$ and $V = U \oplus U^\perp$ also $V = U \oplus U'$ is clear by the definiton of U'. Thus consider any $x \in U^\perp$ and write $x = u + u' \in U + U'$. Then $u' \subseteq U' \subseteq U^\perp$. But as $x = 0 + x \in U + U^\perp$ and the decompositions in $U \oplus U^\perp$ are unique we have $u = 0$ and $u' = x$. In particular $x = u' \in U'$ such that $U^\perp \subseteq U'$ as well. □

Proof of (4.107):

(i) Clearly $P^\top \leq_{\mathsf{m}} M$ is a sub-module of M, as it is the intersection of kernels of a β-linear map and these are sub-modules. Also it is clear that $P \mapsto P^\top$ is order reversing $P_1 \subseteq P_2 \implies P_2^\top \subseteq P_2^\top$ as $P^\top$ is defined by an intersection over $p \in P$. If now $p \in P$ then for any $x \in P^\top$ we have $b(p, x) = 0$. And as this is true for any $x \in P^\top$ we see $p \in (P^\top)^\perp$ such that $P \subseteq (P^\top)^\perp$. Due to the symmetry of the definition the same is true for $Q \mapsto Q^\perp$. Thus $(P \mapsto P^\top, Q \mapsto Q^\perp)$ satisfies property (b) of a Galois connection.

(ii) Consider some $u, v \in L$ and $x, y \in M$ such that $(u + M^\perp, x + L^\top) = (v + M^\perp, y + L^\top)$. That is $v - u \in M^\perp$ and $y - x \in L^\top$. And by definition this implies $b(v - u, y) = 0$ and $b(u, y - x) = 0$ for any $u \in L$ and any $y \in M$. And thereby we find that $\overline{b}$ truly is well-defined (and the linearity in both arguments is trivial), since

$$\begin{aligned} b(v, y) &= b(v - u, y) + b(u, y) = b(u, y) \\ &= b(u, y - x) + b(u, x) = b(u, x) \end{aligned}$$

Also it is clear, that $\overline{b}$ is non-degenerate: Suppose there was some $u + M^\perp \in L/M^\perp$ such that for any $x + L^\top \in M/L^\top$ we had $0 = \overline{b}(u + M^\perp, x + L^\top) = b(u, x)$, then by definition this means $u \in M^\perp$ and hence $u + M^\perp = 0 \in L/M^\perp$. In complete analogy we also find $(M/L^\top)^\perp = 0$ such that $\overline{b}$ is non-degenerate.

(iii) As for any $i \in I$ we have $P_i \subseteq \sum_i P_i$ and $P \mapsto P^\top$ is order-reversing we already have $(\sum_i P_i)^\top \subseteq$

$P_i^\top$ for any $i \in I$. And this is the "$\subseteq$" part of the equality. For the converse inclusion we consider any $x \in M$ with $x \in \bigcap_i P_i^\top$. This means that for any $i \in I$ and any $p_i \in P_i$ we have $b(p_i, x) = 0$. If now $u \in \sum_i P_i$ is any element of the sum of the P_i then (by definition) there is a finite subset $\Omega \subseteq I$ such that $u = \sum_i p_i$ for some $p_i \in P_i$ where the sum runs over $i \in \Omega$. But then we get

$$b(u,x) \;=\; b\left(\sum_{i\in\Omega} p_i, x\right) \;=\; \sum_{i\in\Omega} b(p_i,x) \;=\; \sum_{i\in\Omega} 0 \;=\; 0$$

That is $b(u,x) = 0$ for any $u \in \sum_i P_i$. But by definition this is nothing but $x \in (\sum_i P_i)^\top$ and thereby $\bigcap_i P_i^\top \subseteq (\sum_i P_i)^\top$ as x has been arbitrary. Due to the symmetry the argument it also is clear, that this is true for any family of sumbodules $(Q_j) \subseteq \mathrm{Subm}(M)$.

(iv) Consider any $0 \neq x \in L$ and any $0 \neq y \in M$. If $a \in \mathrm{ann}(x)$ then $ax = 0$ and hence $0 = b(0,y) = b(ax,y) = \alpha(a)b(x,y) = \beta(a)b(x,y) = b(x,ay)$. As $x \neq 0$ but b is integral this implies $ay = 0$ which is $a \in \mathrm{ann}(y)$ again. Hence we have $\mathrm{ann}(x) \subseteq \mathrm{ann}(y)$ and the equality is clear, due to the symmetry of the argument.

It remains to prove, that $\mathrm{ann}(x) \trianglelefteq_{\mathrm{i}} R$ is a prime ideal. First of all we have $x \neq 0$ such that $1 \notin \mathrm{ann}(x)$ and hence $\mathrm{ann}(x) \neq R$. Now consider any two $a, r \in R$ such that $ar \in \mathrm{ann}(x)$ but $r \notin \mathrm{ann}(x)$, then we have to prove $a \in \mathrm{ann}(x)$: Choose any $0 \neq y \in M$, then $0 = b(0,y) = b(arx,y) = \alpha(a)b(rx,y) = \beta(a)b(rx,y) = b(rx,ay)$. But as $r \notin \mathrm{ann}(x)$ we have $rx \neq 0$ and as b is integral this implies $a \in \mathrm{ann}(y) = \mathrm{ann}(x)$. Therefore $\mathrm{ann}(x) \in \mathrm{Spec}(R)$ is a prime ideal.

□

Proof of (4.101):

(i) First of all $\{ m'_1, \ldots, m'_n \}$ is linearly independent: suppose we have a linear relation (for some $a_i \in R$) between the m'_i of the form

$$\sum_{i=1}^{n} a_i\, m'_i \;=\; 0$$

But from this we get $a_j = 0$ for any $j \in 1 \ldots n$ (which is the linear independence, as desired) by evaluating this at $m_j \in M$

$$0 \;=\; \sum_{i=1}^{n} a_i\, m'_i(m_j) \;=\; \sum_{i=1}^{n} a_i\, \delta_{i,j} \;=\; a_j$$

But this set also generates M': Given any $f \in M'$ we let $f_i := f(m_i)$ (hence $f_i \in R$). For any $x = \sum_i x_i m_i \in M$ we then get

$$f(x) \;= f\left(\sum_{i=1}^{n} x_i\, m_i\right) = \sum_{i=1}^{n} x_i\, f_i \;=\; \sum_{i=1}^{n} f_i\, m'_i(x)$$

As this is true for any $x \in M$ we have $f = \sum_i f_i m'_i$ which is contained in the linear hull of the m'_i. Together $\{ m'_1, \ldots, m'_n \}$ is a basis of M'.

(ii) Consider any $f \in M'$ and expand it as $f = \sum_i f_i m'_i$. Then for any $k \in 1 \ldots n$ we find $\beta(m_k)(f) =$

$m''_k(f)$ by computing

$$\begin{aligned}\beta(m_k)\left(\sum_{i=1}^n f_i m'_i\right) &= \sum_{i=1}^n f_i \beta(m_k)(m'_i) = \sum_{i=1}^n f_i m'_i(m_k)\\ &= \sum_{i=1}^n f_i \delta_{i,k} = \sum_{i=1}^n f_i m''_k(m'_i) = m''_k\left(\sum_{i=1}^n f_i m'_i\right)\end{aligned}$$

(iii) Let us first suppose M is free and pick up a basis $\{ m_i \mid i \in I \}$ of M. For any $j \in I$ let us the define $m'_j \in M'$ as with the dual basis

$$m'_j : M \to R : \sum_{i=1}^n a_i m_i \mapsto a_j$$

Then for any $x = \sum_i x_i m_i$ we get $\beta(x)(m'_j) = m'_j(x) = x_j$. Thus $\beta(x) = 0$ implies $x_j = 0$ for any $j \in I$ which means $x = 0$. And as $\mathrm{kn}(\beta) = 0$ we see that β is injective.

If the basis of M is finite $\{ m_1, \ldots, m_n \}$ then by (i) we can take to the dual basis $\{ m'_1, \ldots, m'_n \}$ which is $m'_j(m_i) = \delta_{i,j}$. Using (i) again we can also look at the dual basis of the dual basis $\{ m''_1, \ldots, m''_n \}$ which is $m''_j(m'_i) = \delta_{i,j}$. But thereby we find $\beta(m_i)(m'_j) = m'_j(m_i) = \delta_{i,j} = m''_i(m'_j)$ such that $\beta(m_i)$ and m''_i agree on $\{ m'_1, \ldots, m'_n \}$. But as this generates M' (it even is a basis) this means $\beta(m_i) = m''_i$ such that $M'' = \mathrm{Lh}\{ m''_1, \ldots, m''_n \} \subseteq \mathrm{im}(\beta) \subseteq M''$. But $\mathrm{im}(\beta) = M''$ is the surjectivity of β that we needed.

(iv) For (a) $\implies$ (c) we start with any $x \in M$ such that $f(x) = 0$ for any $f \in M'$. That is $\beta(x)(f) = f(x) = 0$ for any $f \in M'$ which means $\beta(x) = 0 \in M''$. But as β is injective we have $\mathrm{kn}(\beta) = 0$ such that $x = 0$. For (c) $\implies$ (b) we first note that δ is bilinear (by remark (4.100.(iii))) and hence a duality. Now (c) is property (2) of the dual pair. So we have to prove property (3): for any $f \in M'$ we need the implication $(\forall\, x \in M : f(x) = 0) \implies f = 0$. But this is trivial, $f(x) = 0$ for any $x \in M$ means that $f = 0$ is the zero map. It remains (b) $\implies$ (a): If suffices to show $\mathrm{kn}(\beta) = 0$. Thus consider any $x \in M$ with $\beta(x) = 0$, that is $\beta(x)(f) = 0$ for any $f \in M'$. This is $f(x) = \beta(x)(f) = 0$ such that $x = 0$ by property (2) of (M, M').

(v) Property (1) is identical, but we will prove that in this case (2) and (2') resp. (3) and (3') are equivalent: For property (2) this is plain to see $\forall\, f \in \mathrm{im}(\delta) : f(x) = 0$ is just a reformulation of $\forall\, x \in N : \delta_x(u) = 0$. But as $\delta_x(u) = \delta(u, x)$ this is just property (2) again. Let us turn to the implication (3) $\implies$ (3') next: By assumption we have $\forall\, u \in M : \delta_x(u) = 0 \implies x = 0$. In terms of maps this is $\delta_x = 0 \implies x = 0$. Now suppose we had $\delta_x = \delta_y$ then $0 = \delta_y - \delta_x = \delta_{y-x}$ such that $x - y = 0$ and hence $x = y$. And this is the injectivity of $x \mapsto \delta_x$. Conversely (3') $\implies$ (3): Suppose there was some $x \in N$ such that $\forall\, u \in M : \delta_x(u) = 0$. In terms of maps this is $\delta_x = 0$. But as δ is a duality we have $\delta_0 = 0$ already, so by injectivity we get $x = 0$.

(vi) Clearly $S(y) : x \mapsto s(x \mid y)$ is well-defined, by properties (1) and (2) of a sesqui-linear map. Therefore S is well-defined. Also $y \mapsto S(y)$ is ε-linear, by properties (4) and (5) of a sesqui-linear map. For the injectivity of S we consider any two $y, z \in M$ such that $S(y) = S(z)$. Then $0 = S(z - y)$, that is for any $x \in M$ we have $0 = S(z - y)(x) = s(x \mid z - y)$. In particular for

$x = z - y$ we have $0 = s(x \mid x)$. But as s is poritive definite we have $0 = s(x \mid x) \in R^*$ a contradiction. This means $z - y = 0$ and hence $y = z$ which is the injectivity of S.

For the surjectivity of S we pick up an ONB $\{ g_1, \ldots, g_n \}$ of M according to (4.97.(iii)), which is possible, since M is free and finitely generated. Let $\{ g'_1, \ldots, g'_n \}$ be the respective dual basis. Then we claim $S(g_i) = g'_i$ for any $i \in 1 \ldots n$. To do this consider any $x \in M$, as the g_i are a basis of M we get

$$x \;=\; \sum_{i=1}^{n} x_i g_i \quad \text{where} \quad x_i \;=\; s(x \mid g_j)$$

according to (4.97.(ii)). But by definition of the dual base we also have $g'_i(x) = x_i = s(x \mid g_i) = S(g_i)(x)$. As this is true for any x we see $g'_i = S(g_i)$. As the g'_i generate M' we can write any $f \in M'$ as

$$f \;=\; \sum_{i=1}^{n} f_i g'_i$$

for some $f_i \in R$. As ε is surjective we can choose some $a_i \in R$ such that $\varepsilon(a_i) = f_i$. Then we find the surjectivity of S, as

$$S\left(\sum_{i=1}^{n} a_i g_i \right) \;=\; \sum_{i=1}^{n} \varepsilon(a_i)\, S(g_i) \;=\; \sum_{i=1}^{n} f_i g'_i \;=\; f$$

□

Proof of (4.104):

(i) Let $\mathcal{M} = (m_1, \ldots, m_n)$ be the ONB given and recall that the adjoint endomorphism φ' is determined by the following property, for any $x, y \in M$

$$s\big(\varphi(x) \mid y\big) \;=\; s\big(x \mid \varphi'(y)\big)$$

We specifically chose $x = m_i$ and $y = m_k$ for any $i, k \in 1 \ldots n$, then - by construction of the matrix representation - we find the entries of A and A', since

$$\begin{aligned} s\big(\varphi(m_i) \mid m_k\big) \;&=\; s\left(\sum_{j=1}^{n} [A]_{i,j} m_j \mid m_k \right) \;=\; \sum_{j=1}^{n} [A]_{i,j}\, s\big(m_j \mid m_k\big) \;=\; [A]_{i,k} \\ s\big(m_i \mid \varphi'(m_k)\big) \;&=\; s\left(m_i \mid \sum_{j=1}^{n} [A']_{k,j} m_j \right) \;=\; \sum_{j=1}^{n} \varepsilon\big([A']_{k,j}\big) s\big(m_i \mid m_j\big) \;=\; \varepsilon\big([A']_{k,i}\big) \end{aligned}$$

As these are identical, that is $[A^*]_{k,i} = [A]_{i,k} = \varepsilon([A']_{k,i})$ for any $i, k \in 1 \ldots n$ such that $A^* = \varepsilon(A')$. In other words, as ε is invertible, we have $A' = \varepsilon^{-1}(A^*)$, as claimed.

(ii) The implication (a) $\implies$ (b) has already been proved in (4.103.(iii)). And for (b) $\implies$ (c) we recall, that M is a finitely generated free R-module, that is M has a basis $\{ m_1, \ldots, m_n \}$. By Gram-Schmidt-Orthonormalsation (4.97.(iii)) we find an ONB $\{ g_1, \ldots, g_n \}$ of M. Apply any order to this set and call the ordered ONB $\mathcal{G}$. Then (b) provides $A^* = \varepsilon(A)$ for this ONB and hence we have (c). Finally for (c) $\implies$ (a) we have to prove $\varphi' = \varphi$. Yet by (i) we know $A' = \varepsilon^{-1}(A^*)$ and

by assumption $A^* = \varepsilon(A)$ this is

$$A' \;=\; \varepsilon^{-1}\big(A^*\big) \;=\; \varepsilon^{-1}\big(\varepsilon(A)\big) \;=\; A$$

That is $A' = A$ and as $\varphi \mapsto A = [\varphi]_{\mathcal{M}}$ is an isomorphism of R-algebras, this implies $\varphi' = \varphi$. Hence we have come full-circle.

(iii) For (a) $\implies$ (b) we have $\varphi'\varphi = \varphi\varphi'$ and are given any ordered ONB $\mathcal{M}$ of M. As $\varphi \mapsto A = [\varphi]_{\mathcal{M}}$ is an R-algebra isomorphism, using (i) we immediately get

$$\begin{aligned}\big[\varphi'\varphi\big] \;&=\; [\varphi'][\varphi] \;=\; \varepsilon^{-1}\big(A^*\big)\, A\\ \big[\varphi\varphi'\big] \;&=\; [\varphi][\varphi'] \;=\; A\,\varepsilon^{-1}\big(A^*\big)\end{aligned}$$

As $[\varphi'\varphi] = [\varphi\varphi']$ are identical, by (a), we find the identity of the matrices claimed in (b), too. As in (ii) above, (b) implies (c), as there is an (ordered) ONB of M. As for (c) $\implies$ (a), This is just the reverse direction of (a) $\implies$ (b): We can conclude $\varphi'\varphi = \varphi\varphi'$ from the identity of the matrices.

□

Proof of (4.103):

(ii) Suppose $\mathcal{M} = \big\{\, m_1, \ldots, m_p \,\big\}$ is an ONB of M, that is $\mathcal{M}$ is a basis of M such that satisfies $s(m_i, m_j) = \delta_{i,j}$. There is such a basis, since s is positive definite and hence we may use Gram-Schmidt (4.97). Thus if $u \in M^\perp$ then we consider the representation $u = \sum_i u_i m_i$ in this basis and compute

$$0 \;=\; s\big(u \mid m_j\big) \;=\; s\left(\sum_{i=1}^{p} u_i m_i \mid m_j\right) \;=\; \sum_{i=1}^{p} u_i s\big(m_i \mid m_j\big) \;=\; u_j$$

Hence $u \in M^\perp$ implies $u = 0$ and this is $M^\perp = 0$. The same is true for t and hence $N^\perp = 0$, as well.

(i) Clearly $N := R^n$ has the ONB $\big\{\, e_1, \ldots, e_n \,\big\}$ with respect to b_n. That is we have $b_n(e_i, e_j) = \delta_{i,j}$ and hence my use (ii) to find $(R^n)^\perp = 0$ and likewise $(R^m)^\perp = 0$. Then we compute

$$\begin{aligned}\big(\operatorname{im}(A)\big)^\perp \;&=\; \big\{\, u \in R^m \mid \forall\, v \in \operatorname{im}(A) \;:\; \langle u, v\rangle \;=\; 0 \,\big\}\\ &=\; \big\{\, u \in R^m \mid \forall\, y \in R^n \;:\; \langle u, Ay\rangle \;=\; 0 \,\big\}\\ &=\; \big\{\, u \in R^m \mid \forall\, y \in R^n \;:\; \langle A^*u, y\rangle \;=\; 0 \,\big\}\\ &=\; \Big\{\, u \in R^m \mid A^*u \;\in\; \big(R^n\big)^\perp \;=\; 0 \,\Big\} \;=\; \operatorname{kn}\big(A^*\big)\\ \big(\operatorname{im}(A^*)\big)^\perp \;&=\; \big\{\, x \in R^n \mid \forall\, y \in \operatorname{im}(A^*) \;:\; \langle x, y\rangle \;=\; 0 \,\big\}\\ &=\; \big\{\, x \in R^n \mid \forall\, v \in R^m \;:\; \langle x, A^*v\rangle \;=\; 0 \,\big\}\\ &=\; \big\{\, x \in R^n \mid \forall\, v \in R^m \;:\; \langle Ax, v\rangle \;=\; 0 \,\big\}\\ &=\; \Big\{\, x \in R^n \mid Ax \;\in\; \big(R^m\big)^\perp \;=\; 0 \,\Big\} \;=\; \operatorname{kn}\big(A\big)\end{aligned}$$

(iii) Choose ordered ONB $\mathcal{M} = (m_1, \ldots, m_p)$ of M with respect to s and $\mathcal{N} = (n_1, \ldots, n_q)$ of N with respect to t again. And denote the basis representation of φ with respect to these bases by

$A = (a_{j,i}) := [\varphi] \in \mathrm{mat}_{q,p}(R)$, that is $\varphi(m_i) = \sum_j a_{j,i}\, n_j$. Now define $A' = (a'_{i,j}) \in \mathrm{mat}_{p,q}(R)$ by $a'_{i,j} := \varepsilon^{-1}(a_{j,i})$. That is $A' = \varepsilon^{-1}(A^*)$. Then we define $\varphi' : N \to M$ to be the homomorphism which has the representation $A' = [\varphi']$ in these bases, that is $\varphi'(n_j) = \sum_i a'_{i,j}\, m_i$. We claim that φ' is the (one and only) adjoint of φ. That is, given any $u \in M$ and $y \in N$ we need to show $s(u \mid \varphi'(y)) = t(\varphi(u) \mid y)$. If we also represent $[u] = (u_1, \ldots, u_p) \in R^p$ and $[y] = (y_1, \ldots, y_q) \in R^q$ in the respective basis that this boils down to a straightforward computation:

$$\begin{aligned}
s\big(u \mid \varphi'(y)\big) &= s\left(\sum_{i=1}^{p} u_i m_i \mid \sum_{j=1}^{q} y_j \varphi'(n_j)\right) \\
&= \sum_{i=1}^{p}\sum_{j=1}^{q} u_i \varepsilon(y_j)\, s\left(m_i \mid \varphi'(n_j)\right) \\
&= \sum_{i=1}^{p}\sum_{j=1}^{q} u_i \varepsilon(y_j)\, s\left(m_i \mid \sum_{k=1}^{p} a'_{j,k} m_k\right) \\
&= \sum_{i=1}^{p}\sum_{j=1}^{q} u_i \varepsilon(y_j) \sum_{k=1}^{p} \varepsilon(a'_{j,k})\, s(m_i \mid m_k) \\
&= \sum_{i=1}^{p}\sum_{j=1}^{q} u_i \varepsilon(y_j) \sum_{k=1}^{p} \varepsilon\varepsilon^{-1}(a_{k,j})\delta_{i,k} \\
&= \sum_{i=1}^{p}\sum_{j=1}^{q} u_i \varepsilon(y_j) a_{i,j} \\
t\big(\varphi(u) \mid y\big) &= t\left(\sum_{i=1}^{p} u_i \varphi(m_i) \mid \sum_{j=1}^{q} y_j n_j\right) \\
&= \sum_{i=1}^{p}\sum_{j=1}^{q} u_i \varepsilon(y_j)\, t\left(\varphi(m_i) \mid n_j\right) \\
&= \sum_{i=1}^{p}\sum_{j=1}^{q} u_i \varepsilon(y_j)\, t\left(\sum_{k=1}^{q} a_{i,k} n_k \mid n_j\right) \\
&= \sum_{i=1}^{p}\sum_{j=1}^{q} u_i \varepsilon(y_j) \sum_{k=1}^{q} a_{i,k}\, t\left(n_k \mid n_j\right) \\
&= \sum_{i=1}^{p}\sum_{j=1}^{q} u_i \varepsilon(y_j) \sum_{k=1}^{q} a_{i,k}\delta_{k,j} \\
&= \sum_{i=1}^{p}\sum_{j=1}^{q} u_i \varepsilon(y_j) a_{i,j} \\
&= s\big(u \mid \varphi'(y)\big)
\end{aligned}$$

(iii) If φ' is the adjoint homomorphism of φ then by definition we have $t(\varphi(u) \mid y) = s(u \mid \varphi'(y))$. But as both s and t are sesqui-linear forms with respect to ε (the positive definiteness of s or t is not needed)

$$t\big(x \mid \varphi(v)\big) \;=\; \varepsilon\left(t\big(\varphi(v) \mid x\big)\right) \;=\; \varepsilon\left(s\big(v \mid \varphi'(x)\big)\right) \;=\; s\big(\varphi'(x) \mid v\big)$$

(iv) Note that by (ii) we have $M^\perp = 0$ and $N^\perp = 0$. Also note that φ' satisfies both identities of (iii)

Then we simply use the same computation as in (i) before:

$$\begin{aligned}
\big(\mathrm{im}\,(\varphi)\,\big)^{\perp} &= \{\, x \in N \mid \forall\, y \in \mathrm{im}(\varphi) \;:\; t(x \mid y) \,=\, 0 \,\} \\
&= \{\, x \in N \mid \forall\, v \in M \;:\; t(x \mid \varphi(v)) \,=\, 0 \,\} \\
&= \big\{\, x \in N \mid \forall\, v \in M \;:\; s(\varphi'(x) \mid v) \,=\, 0 \,\big\} \\
&= \Big\{\, x \in N \mid \varphi'(x) \,\in\, M^{\perp} \,=\, 0 \,\Big\} \,=\, \mathrm{kn}\big(\varphi'\big) \\
\big(\mathrm{im}\,(A^*)\,\big)^{\perp} &= \big\{\, u \in M \mid \forall\, v \in \mathrm{im}(\varphi') \;:\; s(u \mid v) \,=\, 0 \,\big\} \\
&= \big\{\, u \in M \mid \forall\, y \in N \;:\; s(u \mid \varphi'(y)) \,=\, 0 \,\big\} \\
&= \{\, u \in M \mid \forall\, y \in N \;:\; t(\varphi(u) \mid y) \,=\, 0 \,\} \\
&= \Big\{\, u \in M \mid \varphi(u) \,\in\, \big(N\big)^{\perp} \,=\, 0 \,\Big\} \,=\, \mathrm{kn}\big(\varphi\big)
\end{aligned}$$

□

Proof of (4.110):
The isomorphy of the dual space $(M \oplus N)'$ is just a special case of (3.37). Nevertheless we will give a proof here: First note, that $\pi_M \iota_M : x \mapsto x$ is the identity, whereas $\pi_N \iota_M : x \mapsto 0$ is the zero-map. We also find the following map $\iota_M \pi_M : (x,y) \mapsto (x,0)$. If we start with $h \in (M \oplus N)'$ then

$$h \;\mapsto\; \big(h\iota_M, h\iota_N\big) \;\mapsto\; h\iota_M\pi_M + h\iota_N\pi_N$$

But $h(x,y) = h(x,0) + h(0,y)$, as h is R-linear, so this is h again. Conversely if we start with $(f,g) \in M' \oplus N'$ then this is mapped to

$$(f,g) \;\mapsto\; h := f\pi_M + g\pi_N \;\mapsto\; \big(h\iota_M, h\iota_N\big)$$

Hereby $h\iota_M = f\pi_M\iota_M + g\pi_N\iota_M = f\mathbb{1}_M + g\,0 = f$ and likewise $h\iota_N = g$ again. Thus we have seen that these maps truly are mutually inverse.
Now we turn to the isomorphy of the bidual $(M \oplus N)''$. If we start with $\omega \in (M \oplus N)''$ then this element is mapped to

$$\omega \;\mapsto\; (\omega_M, \omega_N) \;\mapsto\; \big(h \mapsto \omega_M\big(h\iota_M\big) + \omega_N\big(h\iota_N\big)\big)$$

where $\omega_M(f) = \omega(f\pi_M)$ and $\omega_N(g) = \omega(g\pi_N)$. For $f = h\iota_M$ this is $\omega_M(f) = \omega(h\iota_M\pi_M)$ where $h\iota_M\pi_M(x,y) = h(x,0)$. Likewise $h\iota_N\pi_N(x,y) = h(0,y)$ such that the sum of these is $h(x,y)$. This means $h = \omega_M(h\iota_M) + \omega_N(h\iota_N)$ which is the first part. For the second part we start with $\omega_M \in M''$ and $\omega_N \in N''$ such that (ω_M, ω_N) is mapped to ω with

$$\omega(h) \;=\; \omega_M\big(h\iota_M\big) + \omega_N\big(h\iota_N\big)$$

In turn ω is mapped to $f \mapsto \omega(f\pi_M)$ and $g \mapsto \omega(g\pi_N)$ separately. So we need to show $\omega(f\pi_M) = \omega_M(f)$ and $\omega(g\pi_N) = \omega_N(g)$. But watch what ω does to $f\pi_M$

$$\omega\big(f\pi_M\big) \;=\; \omega_M\big(f\pi_M\iota_M\big) + \omega_N\big(f\pi_M\iota_N\big) \;=\; \omega_M(f) + \omega_N(0) \;=\; \omega_M(f)$$

Similarly we find $\omega(g\pi_N) = \omega_N(g)$ such that $(\omega_M, \omega_N) \mapsto \omega \mapsto (\omega_M, \omega_N)$ closes the circle. Together

we have shown the isomorphy of the bidual.
It remains to prove the commutativity of the diagram, that is for any $(x,y) \in M \oplus N$ we need to show $\Theta\beta(x,y) = (\beta_M(x), \beta_N(y))$. Let us abbreviate $\omega := \beta(x,y)$, $\omega_M := \beta_M(x)$ and $\omega_N := \beta_N(y)$, then we need to show $\Theta(\omega) = \omega_M \times \omega_N$. By definition of Θ the M-part of this is $\omega(f\pi_M) = \omega_M(f)$ for any $x \in M$. But then

$$\begin{aligned} \omega(f\pi_M) &= \beta(x,y)(f\pi_M) = f\pi_M(x,y) = f(x) \\ \omega_M(f) &= \beta_M(x)(f) = f(x) \end{aligned}$$

which is $\omega(f\pi_M) = \omega_M(f)$ as needed. Likewise we see $\omega(g\pi_N) = \omega_N(g)$ for any $g \in N'$ which seals the commutativity of the diagram. □

Proof of (4.109):

(i) Consider any $f = \sum_j b_j m'_j \in M'$ and any $p = \sum_i p_i a_i m_i \in P$. Then it is clear, that $f(m_i) = \sum_j b_j m'_j(m_i) = b_i$ and thereby

$$f(p) = \sum_{i=1}^{r} p_i a_i f(m_i) = \sum_{i=1}^{r} p_i a_i b_i$$

Thus if $f \in P^\top$ then $f(p) = 0$ for any $p \in P$ and thereby $a_i bi = 0$ for any $i \in 1 \ldots r$. But as R is an integral domain and $a_i \neq 0$ this implies $b_i = 0$ such that $f \in \mathrm{Lh}\{ m'_{r+1}, \ldots, m'_n \}$. Conversely if $f \in \mathrm{Lh}\{ m'_{r+1}, \ldots, m'_n \}$ then for the same reasoning we have $f(p) = 0$ for any $p \in P$ and hence $f \in P^\top$. Thus we have proved

$$P^\top = \delta(P \mid \perp) = \mathrm{Lh}\{ m'_{r+1}, \ldots, m'_n \}$$

Let us now take a look at $P^{\top\perp} = \delta(\perp \mid P^\top)$ which is defined to be $P^{\top\perp} = \{ x \in M \mid \forall f \in P^\top : f(x) = 0 \}$. If now $f = \sum_j b_j m'_j \in P^\top$ and $x = \sum_k x_k m_k \in M$ then in complete analogy we have

$$f(x) = \sum_{k=1}^{n} x_k f(m_k) = \sum_{j=r+1}^{n} x_j b_j$$

Thus if $x \in \mathrm{Lh}\{ m_1, \ldots, m_r \}$ then $f(x) = 0$ for any $f \in P^\top$ and hence $x \in P^{\top\perp}$. Conversely if $f(x) = 0$ for any $f \in P^{\top\perp}$ then necessarily $x_j = 0$ for any $j \in (r+1) \ldots n$ and hence $x \in \mathrm{Lh}\{ m_1, \ldots, m_r \}$. Thus we also have

$$P^{\top\perp} = \delta(\perp \mid P^\top) = \mathrm{Lh}\{ m_1, \ldots, m_r \}$$

And $\mathrm{Lh}\{ m_1, \ldots, m_r \} = \mathrm{Hull}(P)$ is obvious: By definition any $a_i m_i$ is contained in $\mathrm{Hull}(P)$ (for $i \in 1 \ldots r$) and as these generate P we have $\mathrm{Lh}\{ m_1, \ldots, m_r \} \subseteq \mathrm{Hull}(P)$. Conversely if $x = \sum_k x_k m_k \in M$ such that $ax \in P$ for some $a \in R \setminus \{0\}$, then

$$ax = \sum_{k=1}^{n} a x_k m_k \in P = \mathrm{Lh}\{ a_1 m_1, \ldots, a_r m_r \}$$

As the m_k are a basis of M we may compare coefficients and find $a_i \mid ax_i$ for any $i \in 1 \ldots r$ and

$ax_j = 0$ for $j \in (r+1)\ldots n$. As R is an integral domain and $a \neq 0$ this means $x_j = 0$ and hence $x \in \mathsf{Lh}\{\, m_1, \ldots, m_r \,\}$. Thus we have finally established

$$\mathsf{Lh}\{\, m_1, \ldots, m_r \,\} \;=\; \mathsf{Hull}(P)$$

(ii) As P is a vector space over a field (3.65) tells us, that P is free. Let $\{\, m_1, \ldots, m_r \,\}$ be a basis of P. By (3.64.(v)) we can extend this to a basis $\{\, m_1, \ldots, m_n \,\}$ of M. The identities of $P^\top$ and $P^{\top\perp}$ are just a special case of (i), then.

(iii) Since M is free and finitely generated the natural map $\beta : M \to M''$ is an isomorphism, according to (4.101.(iii)). In particular we have $\beta(M) = M''$ and by definition $x''(f) = f(x)$ for any $x \in M$ and $f \in M'$. But thereby we can just compute

$$\begin{aligned} F^\top &= \{\, \omega \in M'' \mid \forall\, f \in F \,:\, \omega(f) = 0 \,\} \\ &= \{\, x'' \in \beta(M) \mid \forall\, f \in F \,:\, x''(f) = 0 \,\} \\ &= \beta\left(\{\, x \in M \mid \forall\, f \in F \,:\, f(x) = 0 \,\}\right) \\ &= \beta\big(F^\perp\big) \end{aligned}$$

Likewise for $P \leq_{\mathsf{m}} M$ any $\omega \in \beta(P)$ is of the form $\omega = x''$ for some $x \in P$ and thereby $\omega(f) = x''(f) = f(x)$. Thus we find

$$\begin{aligned} \beta(P)^\perp &= \{\, f \in M' \mid \forall\, \omega \in \beta(P) \,:\, \omega(f) = 0 \,\} \\ &= \{\, f \in M' \mid \forall\, x \in P \,:\, f(x) = 0 \,\} \;=\; P^\top \end{aligned}$$

(iv) The implication (a) $\Longrightarrow$ (b) is clear: Just let $Q := \mathsf{Lh}\{\, m_{r+1}, \ldots, m_n \,\}$ then it is clear that $M = P \oplus Q$. For (b) $\Longrightarrow$ (d) we are given $x \in \mathsf{Hull}(P)$, that is $ax \in P$ for some $\in R$ with $a \neq 0$. Write out $x = p + q$ for some $p \in P$ and $q \in Q$, then $ax = ap + aq \in P$. As $M = P \oplus Q$ this means $aq = 0$. But as R is an integral domain (even a PID) and M is free, M also is torsion-free. Thus $aq = 0$ and $a \neq 0$ imply $q = 0$ such that $x = p + q = p \in P$. Thus we have proved $\mathsf{Hull}(P) \subseteq P$ and the converse inclusion is generally true. For the implication (d) $\Longrightarrow$ (e) we note that by assumption and (i) we have $P = \mathsf{Hull}(P) = P^{\top\perp}$. And (e) $\Longrightarrow$ (c) is trivial, as we may just take $F := P^\top \leq_{\mathsf{m}} M'$. It only remains to prove (c) $\Longrightarrow$ (a): So by assumption we have

$$P \;=\; F^\perp \;=\; \{\, x \in M \mid \forall\, f \in F \,:\, f(x) = 0 \,\}$$

Since M is free and finitely generated M' is such, as well, by (4.101.(i)). Since R is a PID (5.28.(iv)) tells us that there are a basis $\{\, f_1, \ldots, f_n \,\}$ of M' and factors $a_1, \ldots, a_r \in R$ such that $\{\, a_1 f_1, \ldots, a_r f_r \,\}$ is a basis of F. Then by (i) we get

$$\begin{aligned} F^\top &= \{\, \omega \in M'' \mid \forall\, f \in F \,:\, \omega(f) = 0 \,\} \\ &= \mathsf{Lh}\{\, f'_{r+1}, \ldots, f'_n \,\} \end{aligned}$$

Again the natural map $\beta : M \xrightarrow{\sim} M''$ is an isomorphism, by (4.101.(iii)). Thus we may take $m_k := \beta^{-1}(f'_k) \in M$ that is $f'_k = m''_k$ for any $k \in 1\ldots n$. Then $\{\, m_1, \ldots, m_n \,\}$ is a basis of M and

by (iii)

$$\begin{aligned}\beta(P) &= \beta\big(F^{\perp}\big) = F^{\top}\\ &= \mathsf{Lh}\{\, f'_{r+1},\ldots,f'_n \,\}\\ &= \mathsf{Lh}\{\, \beta(m_{r+1}),\ldots,\beta(m_n) \,\}\\ &= \beta\big(\mathsf{Lh}\{\, m_{r+1},\ldots,m_n \,\}\big)\end{aligned}$$

As β is injective (even an isomorphism) this implies the equality of $P = \mathsf{Lh}\{\, m_{r+1},\ldots,m_n \,\}$. So by renumbering the basis $\{\, m_1,\ldots,m_n \,\}$ of M we have proved the claim of (a).

(v) For an arbitrary commutative ring we have seen the Galois connection between the sub-modules of M and M' as a special case of (4.107.(i)). And by (0.22) it is a general truth of Galois connections that these interlock the images of the respective maps, that is

$$\begin{array}{ccc}\mathsf{Orc}(M) & \longleftrightarrow & \mathsf{Orc}(M')\\ P & \mapsto & P^{\top}\\ F^{\perp} & \hookleftarrow & F\end{array}$$

where $\mathsf{Orc}(M) := \big\{\, F^{\perp} \mid F \leq_{\mathfrak{m}} M' \,\big\} \subseteq \mathsf{Subm}(M)$ and $\mathsf{Orc}(M') := \big\{\, P^{\top} \mid P \leq_{\mathfrak{m}} M \,\big\} \subseteq \mathsf{Subm}(M')$. But in (iv) we have seen, that $P \in \mathsf{Orc}(M)$ is equivalent to P being a complemented sub-module

$$\mathsf{Orc}(M) = \mathsf{Subc}(M)$$

But as M' is a finitely generated module over a PID R, as well, we can also apply (iv) to a sub-module $F \leq_{\mathfrak{m}} M'$ of M'. That is F is a complemented sub-module of M' if and only if $F = \Omega^{\perp}$ for some $\Omega \leq_{\mathfrak{m}} M''$. But letting $P := \beta^{-1}(\Omega)$ this is $\Omega^{\perp} = \beta(P)^{\perp} = P^{\top}$ due to (iii). Thus we see that $F \in \mathsf{Subc}(M')$ is equivalent to $F \in \mathsf{Orc}(M')$ and thereby we also have

$$\mathsf{Orc}(M') = \mathsf{Subc}(M')$$

□

Proof of (4.111):

(i) Note that $\Theta\beta = \beta_M \times \beta_N$ for some bijective map Θ according to (4.110). Thus if both β_M and β_N are injective then β has to be, as well. Conversely, if β is injective then $\Theta\beta$ is injective, as well and this means both β_M and β_N are injective.

Likewise if β_M and β_N are surjective, then $\beta = \Theta^{-1}(\beta_M \times \beta_N)$ is surjective as well. And if β is surjective then $\Theta\beta$ is surjective, as well and this means both β_M and β_N are surjective.

(ii) This is just a special case of (i): $M \oplus N$ was called *reflexive* iff the natural map β is bijective. And by (i) this is equivalent to β_M and β_N being bijective. But this is when we say M and N are reflexive.

(iii) If P is projective, then there is another R-module Q and a free R-module F such that $F = P \oplus Q$. Since F is free we know that β_F is injective, due to (4.101.(ii)). But then β_P is injective, as well,

according to (i).

Likewise if P if projective and finitely generated, then F can be taken to be finitely generated, too by (??). Thus (4.101.(ii)) tells us, that β_F even is bijective, such that β_P is bijective, by (i). An this means that P is reflexive.

□

Proof of (4.120):

(i) Let us first prove that $\mathrm{Ch}(X)$ is convex: Consider any $x = \sum_i a_i x_i$ and $y = \sum_j b_j y_j$ in $\mathrm{Ch}(X)$. That is x_i and $y_j \in X$ and a_i, $b_j \in \mathbb{R}^+$ where $\sum_i a_i = 1$ and $\sum_j b_j = 1$. If we are now given any a, $b \in \mathbb{R}^+$ such that $a + b = 1$, then

$$ax + by \;=\; \sum_{i=1}^{m} aa_i x_i + \sum_{j=1}^{n} bb_j y_j$$

Thereby aa_i and $bb_j \in \mathbb{R}^+$ and we find that the arbitrary element $ax + by$ of the line segment is contained in $\mathrm{Ch}(X)$ again, since

$$\sum_{i=1}^{m} aa_i + \sum_{j=1}^{n} bb_j \;=\; a\sum_{i=1}^{m} a_i + b\sum_{j=1}^{n} b_j \;=\; a + b \;=\; 1$$

If now $x \in X$ is any fixed element, then we need to prove the identity for $\mathrm{Ch}(X)$. Given $a_k \in \mathbb{R}^+$ with $\sum_k a_k \leq 1$ we let $a_0 := 1 - \sum_k a_k \geq 0$ and $x_0 := x$, then we see that

$$\begin{aligned} x + \sum_{k=1}^{n} a_k(x_k - x) \;&=\; \left(1 - \sum_{k=1}^{n} a_k\right) x + \sum_{k=1}^{n} a_k x_k \\ &=\; a_0 x_0 + \sum_{k=1}^{n} a_k x_k \;\in\; \mathrm{Ch}(X) \end{aligned}$$

is contained in $\mathrm{Ch}(X)$. Conversely consider $z = \sum_k a_k x_k \in \mathrm{Ch}(X)$, that is $\sum_k a_k = 1$. If $x \notin \{x_1, \ldots, x_n\}$ then we find

$$z \;=\; x - \left(\sum_{k=1}^{n} a_k\right) x + \sum_{k=1}^{n} a_k x_k \;=\; x + \sum_{k=1}^{n} a_k(x_k - x)$$

And if $x \in \{x_1, \ldots, x_n\}$ then we may assume $x = x_1$ without loss of generality. And thereby we find another representation of z of the form desired

$$\begin{aligned} z \;&=\; a_1 x + \sum_{k=2}^{n} a_k x_k \\ &=\; a_1 x + \sum_{k=2}^{n} a_k(x_k - x) + \sum_{k=2}^{n} a_k x \\ &=\; \left(\sum_{k=1}^{n} a_k\right) x + \sum_{k=2}^{n} a_k(x_k - x) \\ &=\; x + \sum_{k=2}^{n} a_k(x_k - x) \end{aligned}$$

(ii) Consider any $x, y \in \bigcap_i C_i$ and any $a, b \in \mathbb{R}^+$ such that $a + b = 1$. As $x, y \in C_i$ and C_i is convex, we find $ax + by \in C_i$. But as this is true for any $i \in I$ we have $ax + by \in \bigcap_i C_i$ again.

(iii) The inclusion "$\subseteq$" is easy to see: Of course we have $X \subseteq \mathrm{Ch}(X)$, as for any $x \in X$ we have $x = 1\dot{x} \in \mathrm{Ch}(X)$. But by (i) we also know that $\mathrm{Ch}(X)$ is convex. Thus $C = \mathrm{Ch}(X)$ meets the conditions of the set on the left hand side and hence we have "$\subseteq$".

For the converse inclusion "$\supseteq$" we need to show $\mathrm{Ch}(X) \subseteq C$ for any convex subset $C \subseteq V$ with $X \subseteq C$. Thus consider any $z = \sum_k a_k x_k \in \mathrm{Ch}(X)$, then we will prove $z \in C$ by induction on n: In case $n = 1$ we have $z = a_1 x_1$ for some $a_1 = 1$ and $x_1 \in X$, that is $z = x_1 \in X \subseteq C$. For the induction step $n + 1$ we first note that a_{n+1} would mean $z = a_{n+1} x_{n+1}$ so we are done by the case $n = 1$ already. Next suppose we had $a_{n+1} = 0$. Then we could omit x_{n+1} in $z = a_1 x_1 + \ldots a_n x_n + a_{n+1} x_{n+1}$ such that the sum would run over the first n elements only and we can already use the induction hypothesis to find $z = a_1 x_1 + \ldots a_n x_n \in C$. Thus we may assume $b := a_{n+1} > 0$ and let $a := a_1 + \cdots + a_n$. Then $0 < a = 1 - b < 1$ and therefore we may define $y := x_{n+1}$ and

$$x \;:=\; \sum_{k=1}^{n} \frac{a_k}{a} x_k \;\in\; V$$

As $\sum_k a_k/a = (\sum_k a_k)/a = a/a = 1$ we have $x \in \mathrm{Ch}(X)$ and thereby $x \in C$ by induction hypothesis. Also $y \in X \subseteq C$ by assumption on C. But as C is a convex set and $a + b = 1$ this implies $ax + by \in C$ again. But it is clear that this is z

$$ax + by \;=\; a \sum_{k=1} \frac{a_k}{a} x_k + a_{n+1} x_{n+1} \;=\; \sum_{k=1}^{n+1} \frac{a_k}{a} x_k \;=\; z$$

□

Proof of (4.122):

(i) As $\mathbb{F}$ is a field and the scalar, resp. inner product is a positive definite sesqui-linear form on $\mathbb{F}^n$ we can choose an ONB of $\mathbb{F}^n$ with $U = \mathrm{Lh}\{ g_1, \ldots, g_r \}$ according to (4.98). If now $u \in U$ is any point in U, then we have a basis representation

$$u \;=\; \sum_{k=1}^{r} c_k g_k \;\in\; U$$

We now wish to find the $u \in U$ such that the distance $\| u - x \|$ is minimal. But as the square $\mathbb{R}^+ \to \mathbb{R}^+ : a \mapsto a^2$ preserves order (that is $a < b \iff a^2 < b^2$ it suffices to minimize the following function

$$d(u) \;:=\; \|u - x\|^2$$

As $\mathbb{R} \subseteq \mathbb{C}$ and the inner product agrees with the scalar product for real vectors it suffices to regard $\mathbb{F} = \mathbb{C}$ only. Then

$$\begin{aligned} d(u) &= \langle u - x \mid u - x \rangle \;=\; \langle u \mid u \rangle - \langle u \mid x \rangle - \langle x \mid u \rangle + \langle x \mid x \rangle \\ &= \langle u \mid u \rangle - \big(\overline{\langle x \mid u \rangle} + \langle x \mid u \rangle \big) + \langle x \mid x \rangle \\ &= \langle u \mid u \rangle - 2\mathrm{re}\big(\langle x \mid u \rangle \big) + \langle x \mid x \rangle \end{aligned}$$

Now let $c_k = a_k + ib_k$ and $w_k = u_k + iv_k = \langle x \mid u\rangle$, then we can continue to evaluate this expression by parts

$$\begin{aligned}
\langle u \mid u\rangle &= \langle \sum_{j=1}^{r} c_j g_j \mid \sum_{k=1}^{r} c_k g_k\rangle \\
&= \sum_{j=1}^{r}\sum_{k=1}^{r} c_j \overline{c}_k \langle g_j \mid g_k\rangle \\
&= \sum_{k=1}^{r} c_k \overline{c}_k \;=\; \sum_{k=1}^{r} \left(a_k^2 + b_k^2\right) \\
\langle x \mid u\rangle &= \langle x \mid \sum_{k=1}^{r} c_k g_k\rangle \;=\; \sum_{k=1}^{r} \overline{c}_k \langle x \mid g_k\rangle \;=\; \sum_{k=1}^{r} \overline{c}_k w_k \\
&= \sum_{k=1}^{r} \left(a_k u_k + b_k v_k + i a_k v_k - i b_k u_k\right)
\end{aligned}$$

Thus if we aggregate $a = (a_1, \ldots, a_r)$ resp. $b = (b_1, \ldots, b_r) \in \mathbb{R}^r$ then $d(u) = d(a, b)$ really is a function of the form $d : \mathbb{R}^{2r} \to \mathbb{R}$

$$d(a,b) \;=\; \sum_{k=1}^{r} \left(a_k^2 + b_k^2\right) - 2\sum_{k=1}^{r} \left(a_k u_k + b_k v_k\right) + \|x\|^2$$

In fact d is a quadratic form so it has a uniquely determined minimum, but let us apply some calculus: If (a, b) is a minimum then all the partial derivatives vanish e.g. [Barner, Flohr, Analysis II, Kapitel 14.4]

$$\begin{aligned}
0 \;=\; \frac{\partial}{\partial a_j} f &= -2u_j + 2a_j \\
0 \;=\; \frac{\partial}{\partial b_j} f &= -2v_j + 2b_j
\end{aligned}$$

That is $c_j = a_j + ib_j = u_j + iv_j = w_j = \langle x \mid g_j\rangle$ which means, that the point $u \in U$ of least distance to x has the coefficients $c_k = \langle x \mid g_j\rangle$. In particular it is uniquely determined. And it truly is a minimum, as the Hesse matrix of d is $2 \cdot \mathbb{1}_{2r}$ which is positive definite.

(ii) We need to find the minimum of the function $S \to \mathbb{R}^+ : t \mapsto \| t - x \|$. But as $S = s + U$ where $U = S - s \;\leq_{\mathrm{v}}\; \mathbb{F}^n$ is a subspace of $\mathbb{F}^n$ we can reformulate this to find the minimum of the function

$$d(u) \;=\; \|(s + u) - x\|^2 \;=\; \|(u - (x - s)\|^2$$

where $u \in U$. In (i) we have seen that the point $q \in U$ for which this distance is minimal has the coefficients $c_k = \langle x - s \mid g_k\rangle$, that is

$$q \;=\; \sum_{k=1}^{r} \langle x - s \mid g_k\rangle\, g_k \;\in\; U$$

Thus $p = s + q$ is the point in S that minimizes $\|t - x\|$ for $t \in S$. In other words: $p = s + u$ is the orthogonal projection of x to S.

(iii) This is just the special case $r = 1$ of (ii): Since $u \neq 0$ we may define $g := u/\|u\|$. Then clearly $\langle g \mid g \rangle = 1$ such that $\{ g \}$ is an ONB of $U = S - s = \mathbb{F}u$. And hence we find

$$p \;=\; s + \langle x - s \mid g \rangle\, g \;=\; s + \langle x - s \mid \frac{u}{\|u\|} \rangle\, \frac{u}{\|u\|} \;=\; s + \frac{\langle x - s \mid u \rangle}{\|u\|^2} u$$

□

Proof of (4.123):

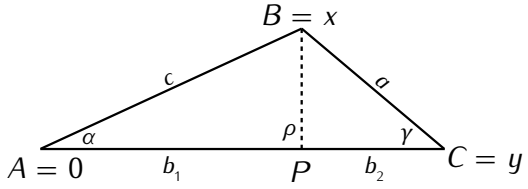
In elementary geometry you have to be extra-careful to distinguish between formal arguments and intuitive insights (that may not convince someone who doesn't share the insight). As we aim to be as rigorous as possible the proof might require more effort than expected. We will rely on the sine rule

$$\frac{\sin(\alpha)}{a} \;=\; \frac{\sin(\beta)}{b} \;=\; \frac{\sin(\gamma)}{c}$$

and prove this along the way. If $x = 0$ or $y = 0$ then we have $0 = 0$ so there is nothing to prove. Otherwise we start with $A = 0$, $B = x \neq 0$ and $C = y \neq 0$ and define $S := \mathbb{R}y \subseteq \mathbb{R}^n$. Then S is a line in $\mathbb{R}^n$ and we may use (4.122.(iii)) to find the projection $p \in \mathbb{R}^n$ of x onto S. By said proposition this is given to be

$$p \;=\; \frac{\langle x, y \rangle}{\|y\|^2} y \quad\Longrightarrow\quad \|p\| = \frac{|\langle x, y \rangle|}{\|y\|^2}\, \|y\| = \frac{|\langle x, y \rangle|}{\|y\|}$$

However we will need to distinguish two cases: $\alpha \leq \pi/2$ first and $\alpha > \pi/2$ second. In the first case the triangle looks like



- Let us first prove the sine rule $c \cdot \sin(\alpha) = a \cdot \sin(\gamma)$: If we choose P such that the angle $\varrho = \pi/2$ is right, then we may use the definition of sine to already find

$$c \cdot \sin(\alpha) \;=\; d \;=\; a \cdot \sin(\gamma)$$

- Note that by construction $p \in \mathbb{R}^n$ is the one point $p \in S$ for which the distance d is minimal. Let us argue, that in this case $\varrho = \pi/2$ is a right angle: By the sine rule applied to ABp we have

$$d \cdot \sin(\varrho) \;=\; c \cdot \sin(\alpha) \quad\Longrightarrow\quad \sin(\varrho) \;=\; \frac{c \cdot \sin(\alpha)}{d}$$

 As $c \cdot \sin(\alpha)$ is fixed and d is as small as it can be, $\sin(\varrho)$ is as large, as it can be, which is $\sin(\varrho) = 1$. And this is the case for a right angle $\varrho = \pi/2$, which also yields $P = p$.

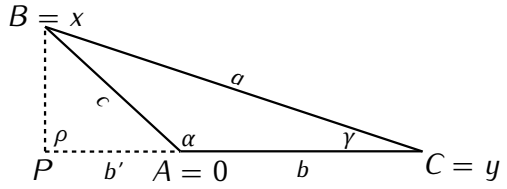
- Then we can use $\|p\|$ and the definition of cosine to compute the angle

$$\cos(\alpha) \;=\; \frac{b_1}{c} \;=\; \frac{\|p\|}{\|x\|} \;=\; \frac{|\langle x, y \rangle|}{\|x\| \cdot \|y\|}$$

As $\alpha \leq \pi/2$ we have it, that P lies in the positive direction of y, when looking from $A = 0$. That is $p = ay$ for some $a > 0$. And as $a = \langle x, y\rangle$ we have $|\langle x, y\rangle| = \langle x, y\rangle$ such that finally

$$\cos(\alpha) \;=\; \frac{\langle x, y\rangle}{\|x\| \cdot \|y\|}$$

So we now turn our attention to the case $\alpha \geq \pi/2$, in this second case the triangle looks a little different



- Again we start by proving the sine rule $c \cdot \sin(\alpha) = a \cdot \sin(\gamma)$ in that case, too: Choose P such that the angle $\varrho = \pi/2$ is right, then by the definition of sine again

 $$c \cdot \sin(\alpha') \;=\; d \;=\; a \cdot \sin(\gamma)$$

 But $\alpha' = \pi - \alpha$ and hence it is clear from the symmetry of the circle in the definition of sine, that $\sin(\alpha') = \sin(\pi - \alpha) = \sin(\alpha)$ such that the sine rule is complete.

- Applying the sine rule to ABp again, we find $P = p$, as before. The proof has been independent of the shape of the triangle.

- This time P lies in the negative direction of y, when looking from A. That is $P = ay$ for some $\langle x, y\rangle = a < 0$ such that $|\langle x, y\rangle| = -\langle x, y\rangle$. And cosine computes the complementary angle $\alpha' = \pi - \alpha$ only

 $$\cos(\alpha') \;=\; \frac{b'}{c} \;=\; \frac{\|p\|}{\|x\|} \;=\; \frac{|\langle x, y\rangle|}{\|x\| \cdot \|y\|}$$

 But from the symmetry of the circle in the definition of cosine it also is clear that $\cos(\alpha') = \cos(\pi - \alpha) = -\cos(\alpha)$ such that we arrive at the same formula, as the minus sign can be scratched

 $$-\cos(\alpha) \;=\; \cos(\alpha') \;=\; \frac{|\langle x, y\rangle|}{\|x\| \cdot \|y\|} \;=\; -\frac{\langle x, y\rangle}{\|x\| \cdot \|y\|}$$

□

Proof of (4.126):
First of all it is straightforward to see, that $\langle a, b\rangle = \langle a, a \wedge x\rangle = 0$ from the definition of the scalar and wedge product:

$$\begin{aligned}
\langle a, a \wedge x\rangle &= a_1(a_2x_3 - a_3x_2) + a_2(a_3x_1 - a_1x_3) + a_3(a_1x_2 - a_2x_1) \\
&= a_1a_2x_3 - a_1a_3x_2 + a_2a_3x_1 - a_1a_2x_3 + a_1a_3x_2 - a_2a_3x_1 \\
&= 0
\end{aligned}$$

Generally we have $a \wedge x = b$ if and only if $b_1 = a_2x_3 - a_3x_2$ and $b_2 = a_3x_1 - a_1x_3$ and $b_3 = a_1x_2 - a_2x_1$. Let us reformulate the third and second equations into $a_1x_2 = b_3 + a_2x_1$ and $a_1x_3 = -b_2 + a_3x_1$

respectively. Then we find, that

$$a_1 x \;=\; \begin{pmatrix} a_1 x_1 \\ a_1 x_2 \\ a_1 x_3 \end{pmatrix} \;=\; \begin{pmatrix} 0 \\ b_3 \\ -b_2 \end{pmatrix} + x_1 \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}$$

This already is the first equation $a_1 x = (0, b_3, -b_1) + x_1 a$ of the claim and in complete analogy we see the other two identities $a_2 x = (-b_3, 0, b_1) + x_2 a$ and $a_3 x = (b_2, -b_1, 0) + x_3 a$. If now $a_1 \in R^*$ is invertible, then we get

$$x \;=\; a_1^{-1} \begin{pmatrix} 0 \\ b_3 \\ -b_2 \end{pmatrix} + (a_1^{-1} x_1) \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \;\in\; \begin{pmatrix} 0 \\ a_1^{-1} b_3 \\ -a_1^{-1} b_2 \end{pmatrix} + Ra$$

Thus we have proved the inclusion $L \subseteq (0, a_1^{-1} b_3, -a_1^{-1} b_1) + Ra$ for the set of solutions $L := \{\, x \in R^3 \mid a \wedge x = b \,\}$. Again, in complete analogy to this case we also find $L \subseteq (-a_2^{-1} b_3, 0, a_2^{-1} b_1) + Ra$ whenever $a_2 \in R^*$ and $L \subseteq (a_3^{-1} b_2, -a_3^{-1} b_1, 0) + Ra$ supposed $a_3 \in R^*$ respectively. It remains to prove the converse inclusions: So let us assume $\langle a, b \rangle = 0$ and $a_1 \in R^*$ and pick up any $u \in R$. Then for $x = (0, a_1^{-1} b_3, -a_1^{-1} b_1) + ua$ we need to show $a \wedge x = b$. First of all it is clear that $a \wedge (b + c) = a \wedge b + a \wedge c$ and $a \wedge a = 0$ such that

$$a \wedge x \;=\; a \wedge \begin{pmatrix} 0 \\ a_1^{-1} b_3 \\ -a_1^{-1} b_2 \end{pmatrix} + u(a \wedge a) \;=\; a \wedge \begin{pmatrix} 0 \\ a_1^{-1} b_3 \\ -a_1^{-1} b_2 \end{pmatrix}$$

And evaluating this expression by the definition of the wedge product finally yields $a \wedge x = b$, using $a_2 b_2 + a_3 b_3 = -a_1 b_1$ in the following computation

$$\begin{aligned} a \wedge x \;&=\; \begin{pmatrix} -a_2 a_1^{-1} b_2 - a_3 a_1^{-1} b_3 \\ a_3 \cdot 0 + a_1 a_1^{-1} b_2 \\ a_1 a_1^{-1} b_3 - a_2 \cdot 0 \end{pmatrix} \;=\; \begin{pmatrix} -a_1^{-1}(a_2 b_2 + a_3 b_3) \\ b_2 \\ b_3 \end{pmatrix} \\ &=\; \begin{pmatrix} -a_1^{-1}(-a_1 b_1) \\ b_2 \\ b_3 \end{pmatrix} \;=\; \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} \;=\; b \end{aligned}$$

In complete analogy we can prove $a \wedge x = b$ for the like cases, in which we have $\langle a, b \rangle = 0$ and $a_2 \in R^*$ or $a_3 \in R^*$ respectively. □

Proof of (4.128):
Properties (1) to (3) and (5) are immediate from the definition of the wedge product. Property (4) is immediate from (6) as $\langle x \wedge y, x \rangle = \det(x, y, x) = 0$ and $\langle x \wedge y, y \rangle = \det(x, y, y) = 0$. So we start with (6) which is a straightforward computation: Let $n := x \wedge y$ that is $n_1 = x_2 y_3 - x_3 y_2$, $n_2 = x_3 y_1 - x_1 y_3$ and $n_3 = x_1 y_2 - x_2 y_1$ then

$$\begin{aligned} \langle x \wedge y, z \rangle \;&=\; n_1 z_1 + n_2 z_2 + n_3 z_3 \\ &=\; x_2 y_3 z_1 - x_3 y_2 z_1 + x_3 y_1 z_2 \\ &\quad\; - x_1 y_3 z_2 + x_1 y_2 z_3 - x_2 y_1 z_3 \end{aligned}$$

$$
\begin{aligned}
&= x_1y_2z_3 + x_2y_3z_1 + x_3y_1z_2 \\
&\quad -x_2y_1z_3 - x_3y_2z_1 - x_1y_3z_2 \\
&= \det(x\ y\ z)
\end{aligned}
$$

We will show (7) by another direct computation, let $n := x \wedge y$ again, then

$$
\begin{aligned}
(x \wedge y) \wedge z &= \begin{pmatrix} n_2z_3 - n_3z_2 \\ n_3z_1 - n_1z_3 \\ n_1z_2 - n_2z_1 \end{pmatrix} \\
&= \begin{pmatrix} x_3y_1z_3 - x_1y_3z_3 - x_1y_2z_2 + x_2y_1z_2 \\ x_1y_2z_1 - x_2y_1z_1 - x_2y_3z_3 + x_3y_2z_3 \\ x_2y_3z_2 - x_3y_2z_2 - x_3y_1z_1 + x_1y_3z_1 \end{pmatrix} \\
\langle x,z\rangle y &= \begin{pmatrix} x_1z_1y_1 + x_2z_2y_1 + x_3z_3y_1 \\ x_1z_1y_2 + x_2z_2y_2 + x_3z_3y_2 \\ x_1z_1y_3 + x_2z_2y_3 + x_3z_3y_3 \end{pmatrix} \\
&= \begin{pmatrix} x_1y_1z_1 + x_2y_1z_2 + x_3y_1z_3 \\ x_1y_2z_1 + x_2y_2z_2 + x_3y_2z_3 \\ x_1y_3z_1 + x_2y_3z_2 + x_3y_3z_3 \end{pmatrix} \\
\langle y,z\rangle x &= \begin{pmatrix} y_1z_1x_1 + y_2z_2x_1 + y_3z_3x_1 \\ y_1z_1x_2 + y_2z_2x_2 + y_3z_3x_2 \\ y_1z_1x_3 + y_2z_2x_3 + y_3z_3x_3 \end{pmatrix} \\
&= \begin{pmatrix} x_1y_1z_1 + x_1y_2z_2 + y_1y_3z_3 \\ x_2y_1z_1 + x_2y_2z_2 + x_2y_3z_3 \\ x_3y_1z_1 + x_3y_2z_2 + x_3y_3z_3 \end{pmatrix}
\end{aligned}
$$

From these we find $(x \wedge y) \wedge z = \langle x,z\rangle y - \langle y,z\rangle x$ and thereby $x \wedge (y \wedge z) = -(y \wedge z) \wedge x = -\langle y,x\rangle z + \langle z,x\rangle y = \langle x,z\rangle y - \langle x,y\rangle z$. Now (8) is an immediate consequence of (7): Clearly the following terms sum up to zero:

$$
\begin{aligned}
x \wedge (y \wedge z) &= \langle x,z\rangle y - \langle x,y\rangle z \\
y \wedge (z \wedge x) &= \langle y,x\rangle z - \langle y,z\rangle y \\
z \wedge (x \wedge y) &= \langle z,y\rangle x - \langle z,x\rangle z
\end{aligned}
$$

For property (9) convince yourself that the k-th coefficient of $x \wedge y$ can be expressed in the following way: For $k \in 1\ldots3$ pick up $i, j \in 1\ldots3$ such that $i < j$ and $\{\, i,j,k \,\} = 1\ldots3$, then

$$
[x \wedge y]_k = (-1)^{k+1}(x_iy_j - x_jy_i)
$$

That is for $k = 1$ we have $(i,j) = (2,3)$, for $k = 2$ we have $(i,j) = (1,3)$ and for $k = 3$ we have $(i,j) = (1,2)$. Hence in the scalar product $\langle u \wedge v, x \wedge y\rangle$ the signs $(-1)^{k+1}$ cancel each other and the

sum $k = 1$ to 3 turns into the sum over $(i,j) \in (1\ldots3)^2$ with $i < j$

$$\begin{aligned}\langle u \wedge v, x \wedge y\rangle &= \sum_{k=1}^{3} [u \wedge v]_k \, [x \wedge y]_k \\ &= \sum_{i<j} (u_i v_j - u_j v_i)\,(x_i y_j - x_j y_i)\end{aligned}$$

So let us check what we find for $\langle u,x\rangle\langle v,y\rangle - \langle u,y\rangle\langle v,x\rangle$, if we evaluate this expression we see that for $i = j$ the terms in the difference cancel each other, such that we can split the sum into two parts again

$$\begin{aligned}&\langle u,x\rangle\langle v,y\rangle - \langle u,y\rangle\langle v,x\rangle \\ = \;& \left(\sum_{i=1}^{3} u_i x_i\right)\left(\sum_{j=1}^{3} v_j y_j\right) - \left(\sum_{i=1}^{3} u_i y_i\right)\left(\sum_{j=1}^{3} v_j x_j\right) \\ = \;& \sum_{i=1}^{3}\sum_{j=1}^{3} \left(u_i x_i v_j y_j - u_i y_i v_j x_j\right) \\ = \;& \sum_{i\neq j} u_i v_j \big(x_i y_j - y_i x_j\big) \\ = \;& \sum_{i<j} u_i v_j \big(x_i y_j - y_i x_j\big) + \sum_{i>j} u_i v_j \big(x_i y_j - y_i x_j\big)\end{aligned}$$

The bracket in the sum over $i > j$ is symmetric in i and j up to sign. Thus if we interchange i and j in this sum we pick up a minus:

$$\begin{aligned}&\langle u,x\rangle\langle v,y\rangle - \langle u,y\rangle\langle v,x\rangle \\ = \;& \sum_{i<j} u_i v_j \big(x_i y_j - y_i x_j\big) - \sum_{i<j} u_j v_i \big(x_i y_j - y_i x_j\big) \\ = \;& \sum_{i<j} \big(u_i v_j - u_j v_i\big)\big(x_i y_j - y_i x_j\big) \\ = \;& \langle u \wedge v, x \wedge y\rangle\end{aligned}$$

To prove property (10) we take a look at the matrix A having the columns x and y, that is $A = (x\,y) \in \mathrm{mat}_{3,2}(\mathbb{R})$. By definition of the column-rank we have c-rank$(A) = 2$ if and only if $\{\,x, y\,\}$ is linear independent. But as $\mathbb{R}$ is an integral domain (even a field) we have c-rank(A) = m-rank(A) due to (4.86) and the (2×2)-minors of A are given to be $m_1 = x_1y_2 - x_2y_1$, $m_2 = x_1y_3 - x_3y_1$ and $m_3 = x_2y_3 - x_3y_2$. That is the wedge product $x \wedge y = (m_3, m_2, m_1)$ contains precisely these minors. In particular we have m-rank$(A) = 2$ if and only if $x \wedge y \neq 0$.

For we next part we take a look at the cofactor matrix first. By it's definition for any $n \in R^3$ the i-th coefficient of $\mathrm{cof}(A)\,n$ is

$$[\mathrm{cof}(A)\,n]_i \;=\; \sum_{j=1}^{3} (-1)^{i+j} \det\big(A_{i,j}\big)\, n_j$$

Let $B := (0,x,y) \in \mathrm{mat}_3(R)$ be the matrix with the columns 0, x and y. Then $AB = (0, Ax, Ay)$ is the matrix with the columns 0, Ax and Ay. Also it is easy to see, that

$$\det\big(B_{1,1}\big) \;=\; x_2y_3 - x_3y_2 \;=\; [x \wedge y]_1$$

$$\begin{aligned}\det(B_{2,1}) &= x_1y_3 - x_3y_1 = -[x \wedge y]_2\\ \det(B_{3,1}) &= x_1y_2 - x_2y_1 = [x \wedge y]_3\end{aligned}$$

We will look at the components of $Ax \wedge Ay$ one by one: We may use property (5) to extract the first coefficient of $Ax \wedge Ay$ as a determinant

$$\begin{aligned}[Ax \wedge Ay]_1 &= \langle e_1, Ax \wedge Ay\rangle = \det(e_1, Ax, Ay)\\ &= 1 \cdot \det\begin{pmatrix}[Ax]_2 & [Ay]_2\\ [Ax]_3 & [Ay]_3\end{pmatrix} = \det\big((AB)_{1,1}\big)\end{aligned}$$

Let $n := x \wedge y$ again. We now apply the formula of Cauchy-Binet to AB, where we choose $\alpha = (2,3)$ and $\gamma = (2,3) \in \mathrm{Asc}(2,3)$. Then

$$\det\big((AB)_{1,1}\big) = \det\big(AB[\alpha \mid \gamma]\big) = \sum_{\beta \in \mathrm{Asc}(2,3)} \det\big(A[\alpha \mid \beta]\big)\det\big(B[\beta \mid \gamma]\big)$$

Note that the sum over $\beta \in \mathrm{Asc}(2,3)$ runs over $(1,2)$, $(1,3)$ and $(2,3)$ which are the complements of 3, 2 and 1 respectively, that is

$$\begin{aligned}[Ax \wedge Ay]_1 &= \det\big((AB)_{1,1}\big) = \sum_{j=1}^{3} \det\big(A_{1,j}\big)\det\big(B_{j,1}\big)\\ &= \det\big(A_{1,1}\big)\, n_1 - \det\big(A_{1,2}\big)\, n_2 + \det\big(A_{1,3}\big)\, n_3\\ &= [\mathrm{cof}(A)\, n]_1\end{aligned}$$

In the same way we are able to prove $[Ax \wedge Ay]_2 = -\det((AB)_{1,2})$ and by choosing $\alpha = (1,3)$ we get $\det((AB)_{1,2}) = -[\mathrm{cof}(A)\, n]_2$. And lastly (with $\alpha = (1,2)$) also $[Ax \wedge Ay]_3 = \det((AB)_{1,3})$ and $\det((AB)_{1,3}) = [\mathrm{cof}(A)\, n]_3$. As we have the equality for any component this finally is

$$Ax \wedge Ay = \mathrm{cof}(A)\, n = \mathrm{cof}(A)\, (x \wedge y)$$

Now we are up to the geometric properties of the wedge product: Let us denote the parallelogram spanned by x and y by $P := \mathrm{Ph}\{\, x, y\,\}$ and the parallelepiped spanned by x, y and z by $Q := \mathrm{Ph}\{\, x, y, z\,\}$. In order to prove $\|x \wedge y\| = \mathrm{Area}(P)$ we use property (9) of the wedge product with $u = x$ and $v = y$. If α is the angle between x and y then we use (4.123) to compute

$$\begin{aligned}\|x \wedge y\|^2 &= \langle x \wedge y, x \wedge y\rangle = \langle x, x\rangle \cdot \langle y, y\rangle - \langle x, y\rangle \cdot \langle y, x\rangle\\ &= \|x\|^2 \cdot \|y\|^2 - (\langle x, y\rangle)^2\\ &= \|x\|^2 \cdot \|y\|^2 - \|x\|^2 \cdot \|y\|^2 \cdot \cos(\alpha)^2\\ &= \|x\|^2 \cdot \|y\|^2 \cdot \big(1 - \cos(\alpha)^2\big)\\ &= \|x\|^2 \cdot \|y\|^2 \cdot \sin(\alpha)^2\end{aligned}$$

Note that for any $\alpha \in [0, \pi]$ the sine $\sin(\alpha) \geq 0$ is positive. Thus we may simply scratch the square from

this equation to find the formula of the area

$$\|x \wedge y\| \;=\; \|x\| \cdot \|y\| \cdot \sin(\alpha) \;=\; \text{Area}(P)$$

For the final formula of the volume, note that $x \wedge y$ is perpendicular to both x and y, according to property (4). That is $x \wedge y$ is perpendicular to the plane P lies in and thereby the angle between $x \wedge y$ and z is $\pi/2 - \beta$. Thus (4.123) again tells us

$$\begin{aligned}
\langle x \wedge y, z \rangle &= \|x \wedge y\| \cdot \|z\| \cdot \cos(\pi/2 - \beta) \\
&= \|x \wedge y\| \cdot \|z\| \cdot \sin(\beta) \\
&= \text{Area}(P) \cdot \|z\| \cdot \sin(\beta) \\
&= \text{Vol}(Q)
\end{aligned}$$

□

Proof of (4.130):
We find from the figure in (4.130), that the trapezoid $T = ABCD$ can be decomposed into two triangles ABD and BCD and hence its area is $\text{Area}(T) = \text{Area}(ABD) + \text{Area}(BCD)$. Let us denote $u := B - A$, $v := D - A$, $x := B - C$ and $y := D - C$. Then our assumption of a trapezoid amounts to $-y = C - D = t(B - A) = tu$ and therefore $x \wedge y = -tx \wedge u = tu \wedge x$. Also $u + x + y = B - A + C - B + D - C = D - A = v$ is clear and hence

$$\begin{aligned}
u \wedge v &= u \wedge (u + x + y) \;=\; u \wedge u + u \wedge x + u \wedge y \\
&= 0 + u \wedge x + 0 \;=\; u \wedge x
\end{aligned}$$

As $x \wedge y = tu \wedge x = tu \wedge v$ we find $\text{Area}(BCD) = (1/2) \;\| x \wedge y \| = (t/2) \;\| u \wedge v \|$ and therefore $\text{Area}(T) = \text{Area}(ABD) + \text{Area}(BCD) = (1 + t)/2 \;\|u \wedge v\|$. But we get the same result for

$$\begin{aligned}
\Big((B - A) + (C - D)\Big) \wedge (C - A) &= (u - y) \wedge (v - y) \\
&= u \wedge v - u \wedge y - y \wedge v + y \wedge y \\
&= u \wedge v + v \wedge y = u \wedge v + x \wedge y \\
&= (1 + t) u \wedge v
\end{aligned}$$

and hence the claim $\text{Area}(T) = (1 + t)/2 \;\|u \wedge v\| = (1/2) \;\|(u - y) \wedge (v - y)\|$. □

Proof of (4.131):
Let us denote $U := \text{Lh}\{\, u, v \,\}$ and $S := s + U$. Define $n := u \wedge v$ and $h := \langle n, s \rangle$ as in the theorem and denote $N := \big\{\, x \in \mathbb{R}^3 \mid \langle n, x \rangle = h \,\big\}$. Then we need to show $S = N$. The inclusion $S \subseteq N$ is easy: If $x \in S$, then x is of the form $x = s + au + bv$ for some a, $b \in \mathbb{R}$. But by (4.128.(3)) we have $\langle n, u \rangle = 0$ and $\langle n, v \rangle = 0$ such that

$$\langle n, x \rangle \;=\; \langle n, s + au + bv \rangle \;=\; \langle n, s \rangle + a \cdot \langle n, u \rangle + b \cdot \langle n, v \rangle \;=\; \langle n, s \rangle \;=\; h$$

which is $x \in N$ already. For the converse inclusion $N \subseteq S$ we look at the map $f : \mathbb{R}^3 \to \mathbb{R} : x \mapsto \langle n, x \rangle$. As $\{\, u, v \,\}$ is linear independent we have $n \neq 0$, due to property (10) of the wedge-product. Thus $f \neq 0$

and thereby $\dim(\mathrm{im}(f)) = 1$. The dimension formula (3.68.(iii)) then implies

$$\dim(\mathrm{kn}(f)) \;=\; \dim(\mathbb{R}^3) - \dim(\mathrm{im}(f)) \;=\; 3-1 \;=\; 2$$

So $P := \mathrm{kn}(f) = \{\, x \in \mathbb{R}^3 \mid \langle n, x\rangle = 0 \,\}$ is 2-dimensional. But as $f(u) = \langle n, u\rangle = 0$ and $f(v) = \langle n, v\rangle = 0$ we already have $U \subseteq P$. If there was some $p \in P \setminus U$, then $\{\, u, v, p \,\} \subseteq P$ were linearly independent which cannot be, as $\dim(P) = 2$. Thus we have $U = P$. We will finally show $N = s + P$. To see this consider any $x \in \mathbb{R}^3$, then $x \in N$ is equivalent, to $f(x) = \langle n, x\rangle = h = \langle n, s\rangle = f(s)$ which is equivalent to $f(x - s) = 0$ which is equivalent to $x - s \in P$ which finally is equivalent to $x \in s + P$. Thus we have $N = s + P$ and thereby $S = s + U = s + P = N$. □

Proof of (5.36):
If $a_j = \lambda$ then $\varphi(m_j) = a_j m_j$ turns into $\varphi(m_j) = \lambda m_j$ and hence $m_j \in \mathrm{Eig}_\varphi(\lambda)$. For the converse incluison we need to verify, that any $x \in \mathrm{Eig}_\varphi(\lambda)$ is a linear combination of those m_j such that $a_j = \lambda$. But as $\{\, m_1, \ldots, m_n \,\}$ is a basis we may write

$$x \;=\; \sum_{j=1}^{n} x_j m_j$$

for some $x_j \in R$. Now apply φ to x, on one side we have $\varphi(x) = \lambda x$, as $x \in \mathrm{Eig}_\varphi(\lambda)$. On the other side φ is R-linear and any $x_j m_j$ is mapped to $x_j a_j m_j$ by assumption on φ. That is we find the identity

$$\lambda x \;=\; \varphi(x) \quad\Longrightarrow\quad \sum_{j=1}^{n} \lambda x_j m_j \;=\; \sum_{j=1}^{n} x_j a_j m_j$$

Subtracting the sums, and using the fact, that the m_j are linearly independent, we get $(a_j - \lambda)x_j = 0$ for any $j \in 1 \ldots n$. As R is an integral domain we get $a_j = \lambda$ or $x_j = 0$ for any $j \in 1 \ldots n$. That is

$$x \;\in\; \mathrm{Lh}\{\, m_j \mid j \in 1 \ldots n,\, a_j = \lambda \,\}$$

as all the x_j with $a_j \neq \lambda$ have to be zero. As we started with an arbitrary $x \in \mathrm{Eig}_\varphi(\lambda)$ this also proves the converse inclusion and hence $\mathrm{Eig}_\varphi(\lambda)$ and $\mathrm{Lh}\{\, m_j \mid j \in 1 \ldots n,\, a_j = \lambda \,\}$ are identical. □

Proof of (5.37):

(i) Clearly the sum and intersection of the P_i are sub-modules of M, by (3.27.(ii)) and (3.10) respectively. It remains to prove the invariance under φ: (1) Consider any $x \in \sum_i P_i$ that is x is a finite sum of elements $x_i \in P_i$. Formally there is a finite subset $\Omega \subseteq I$ and $x_i \in P_i$ (where $i \in \Omega$) such that

$$x \;=\; \sum_{i\in\Omega} x_i \quad\Longrightarrow\quad \varphi(x) \;=\; \sum_{i\in\Omega} \varphi(x_i)$$

As $x_i \in P_i$ and P_i is φ-invariant, we have $\varphi(x_i) \in P_i$ again. And from this we see, that $\varphi(x)$ is contained in $\sum_i P_i$ again. (2) Consider any $x \in \bigcap_i P_i$ that is $x \in P_i$ for any $i \in I$. As P_i is φ-invariant we find $\varphi(x_i) \in P_i$ again (for any $i \in i$) and hence $\varphi(x) \in \bigcap_i P_i$ again.

(ii) Since R is commutative $x \mapsto \pi - \lambda\mathbb{1}$ is a linear map. And therefore $\mathrm{Eig}_\varphi(\lambda) \;\leq_{\mathtt{m}}\; M$ is a sub-module, since it is the kernel of this map $\varphi - \lambda\mathbb{1} \in \mathrm{end}(M)$. It remains to prove that $\mathrm{Eig}_\varphi(\lambda)$ also

is invariant under φ. To do this consider any $x \in \mathrm{Eig}_\varphi(\lambda)$, then we have $\varphi(x) = \lambda x \in \mathrm{Eig}_\varphi(\lambda)$ again, as $\mathrm{Eig}_\varphi(\lambda)$ is a sub-module.

Now, if M is torsion free, then we continue: By definition $ax \in \mathrm{Eig}_\varphi(\lambda)$ means $\varphi(ax) = \lambda ax$. On the other hand we have $\varphi(ax) = a\varphi(x)$ such that a $\varphi(x) = \lambda ax$. As R is commutative, this is $a(\varphi(x) - \lambda x) = 0$. Now, as M is torsion free, this implies $\varphi(x) = \lambda x$, which is $x \in \mathrm{Eig}_\varphi(\lambda)$ again.

(iii) Since M is free and finitely generated $d(\lambda) := \det(\varphi - \lambda \mathbb{1}_M)$ is well-defined. By definition of the spectrum $\lambda \in \mathrm{Spec}(\varphi)$ if and only if $\ker(\varphi - \lambda \mathbb{1}_M) \neq 0$. But since R is an integral domain (4.65.(ii)) tells us that this is the case if and only if $d(\lambda) = 0$.

(iv) We will prove the statement by induction on n: For $n = 1$ we consider some $a_1 x_1 = 0$. As $x_1 \neq 0$ by assumption and M is torsion-free we get $a_1 = 0$ and hence $\{ x_1 \}$ is linearly independent. For the induction step $n \to n+1$ we consider

$$\sum_{i=1}^{n+1} a_i x_i \;=\; 0 \quad\Longrightarrow\quad a_{n+1} x_{n+1} \;=\; -\sum_{i=1}^{n} a_i x_i$$

$$\begin{aligned}
\varphi(a_{n+1}x_{n+1}) &= a_{n+1}\varphi(x_{n+1}) \;=\; a_{n+1}\lambda_{n+1}x_{n+1} \\
&= \lambda_{n+1}a_{n+1}x_{n+1} \;=\; -\lambda_{n+1}\sum_{i=1}^{n} a_i x_i \\
&= -\sum_{i=1}^{n} a_i \lambda_{n+1} x_i \\
\varphi(a_{n+1}x_{n+1}) &= \varphi\left(-\sum_{i=1}^{n} a_i x_i\right) \;=\; -\sum_{i=1}^{n} a_i \varphi(x_i) \\
&= -\sum_{i=1}^{n} a_i \lambda_i x_i
\end{aligned}$$

Thus since we have found two separate expressions for $\varphi(a_{n+1}x_{n+1})$ these have to be equal. And thereby we arrive at a new equation

$$\Longrightarrow\quad -\sum_{i=1}^{n} a_i \lambda_{n+1} x_i \;=\; -\sum_{i=1}^{n} a_i \lambda_i x_i$$

$$\Longrightarrow\quad \sum_{i=1}^{n} a_i \left(\lambda_{n+1} - \lambda_i\right) x_i \;=\; 0$$

By induction hypothesis $\{ x_1, \ldots, x_n \}$ are linearly independent such that we conclude $a_i(\lambda_{n+1} - \lambda_i) = 0$ for any $i \in 1 \ldots n$. But since the λ_i are pairwise distinct we have $\lambda_{n+1} - \lambda_i \neq 0$ and as R is an integral domain this implies $a_i = 0$ for any $i \in 1 \ldots n$. But from this we also see $a_{n+1}x_{n+1} = 0$ and as $x_{n+1} \neq 0$ we conclude $a_{n+1} = 0$, as well. That is $x_1, \ldots, x_n, x_{n+1}$ is linearly independent.

(v) Consider any finite collection of elements $u_{i,j} \in U_i$ where $i \in 1 \ldots n$ and $j \in 1 \ldots m(i)$. If now $a_{i,j} \in R$ are any scalars, then we claimed

$$\sum_{i=1}^{n} \sum_{j=1}^{m(j)} a_{i,j}\, u_{i,j} \;=\; 0 \quad\Longrightarrow\quad \forall\, i \in 1 \ldots n, \forall\, j \in 1 \ldots m(i) \;:\; a_{i,j} \;=\; 0$$

To see this let $u_i := \sum_j a_{i,j}\, u_{i,j}$, as any $u_{i,j} \in U_i \subseteq \mathrm{Eig}_{\lambda_i}(\varphi)$ and the eigenspaces are sub-module of M by (ii) we find that $u_i \in \mathrm{Eig}_{\lambda_i}(\varphi)$. Suppose $u_i \neq 0$ for some $i \in 1 \dots n$, as $u_1 + \dots + u_n = 0$ by assumption this would imply $1 = 0$ due (iv). But as $R \neq 0$ this is not the case. Therefore we have $u_i = 0$ for all $i \in 1 \dots n$. Now

$$u_i \;=\; \sum_{j=1} a_{i,j}\, u_{i,j} \;=\; 0 \quad \Longrightarrow \quad \forall\, j \in 1 \dots m(i) \;:\; a_{i,j} \;=\; 0$$

since all the U_i were supposed to be linearly independent. That is we have $a_{i,j} = 0$ for any $j \in 1 \dots m(i)$ and this for any $i \in 1 \dots n$.

□

Proof of (5.43):
Items (i), (ii), (iv) and (v) are clear, we only have to prove the remaining statements (ii), (iii) and (vi): But (iii) is covered in (4.58.(iii)) and this also yields $c_A(t)$ in (ii), as for $A = \mathrm{dia}(a_1, \dots, n_n)$ we find

$$c_A(t) \;=\; \prod_{j=1}^{n}(t - a_j) \;=\; \prod_{i=1}^{r}(t - \lambda_i)^{k(i)}$$

For the minimal polynomial m_A we assume R to be a noetherian integral domain. Note that, as A is a diagonal matrix, for any $f \in R[t]$ we have $f(A) = \mathrm{dia}(f(a_1), \dots, f(a_n))$. In particular

$$m_A(A) \;=\; \mathrm{dia}\left(\prod_{i=1}^{r}(a_1 - \lambda_i), \dots, \prod_{i=1}^{r}(a_n - \lambda_i)\right) \;=\; \mathrm{dia}(0, \dots, 0) \;=\; 0$$

Also m_A is monic by construction, so it only remains to prove property (3), which is $f(A) = 0$ implies $m_A \mid f$. The assumption $0 = f(A) = \mathrm{dia}(f(a_1), \dots, f(a_n))$ means $f(a_j) = 0$ for any $j \in 1 \dots n$. As $f(t) = q(t) \cdot (t - a_j) + f(a_j)$ (by division with remainder) we hence find $t - a_j \mid f$. In particular $t - \lambda_i \mid f$ for any $i \in 1 \dots r$. But then the $t - \lambda_i$ are pairwise non-associate prime elements of $R[t]$, that all divide f. In other words $\langle t - \lambda_i \mid f \rangle \geq 1$. And thereby (2.59.(vi)) implies

$$m_A \;=\; \prod_{i=1}^{r}(t - \lambda_i) \;\mid\; \prod_{i=1}^{r}(t - \lambda_i)^{\langle t - \lambda_i | f \rangle} \;\mid\; f$$

The proof of (vi) splits into two parts: First we need to show that the characteristic polynomial $c_C(t)$ of the companion matrix $C := \mathrm{comp}(f)$ truly is f again. This is not hard, using induction on the degree n of f: For $n = 1$ we have $f = t + a_0$ and $C = (-a_0)$ a (1×1)-matrix. For this it is clear, that

$$\det(t\mathbb{1}_1 - C) \;=\; \det(t + a_0) \;=\; t + a_0 \;=\; f(t)$$

For the induction step, we have to regard the polynomial $f(t) = t^{n+1} + a_n t^n + \dots + a_1 t + a_0$. To evaluate

the charactristic polynomial of $C = \mathrm{comp}(f)$ we then use Laplace expansion along the first row

$$\det(t\mathbb{1}_{n+1} - C) \;=\; \det\begin{pmatrix} t & 0 & 0 & \cdots & 0 & a_0 \\ -1 & t & 0 & \cdots & 0 & a_1 \\ 0 & -1 & t & & 0 & a_2 \\ \vdots & & -1 & \ddots & & \vdots \\ \vdots & & & \ddots & t & a_{n-1} \\ 0 & 0 & 0 & & -1 & t + a_n \end{pmatrix} \;=\; t \cdot D_1 + (-1)^{n+1+1} a_0 \cdot D_{n+1}$$

Here we still have to take a closer look at the determinants D_1 and D_{n+1} of $n \times n$-matrices: Define the monic polynomial $f_1(t) := t^n + a_n t^{n-1} + \ldots a_2 t + a_1$ and let $C_1 := \mathrm{comp}(f_1)$, then we find

$$D_1 \;:=\; \det\begin{pmatrix} t & 0 & \cdots & 0 & a_1 \\ -1 & t & \cdots & 0 & a_2 \\ \vdots & -1 & \ddots & & \vdots \\ \vdots & & \ddots & t & a_{n-1} \\ 0 & 0 & & -1 & t + a_n \end{pmatrix} \;=\; \det(t\mathbb{1}_n - C_1)$$

$$D_{n+1} \;:=\; \begin{pmatrix} -1 & t & & 0 & 0 \\ 0 & -1 & \ddots & & 0 \\ \vdots & 0 & \ddots & \ddots & \vdots \\ \vdots & & & -1 & t \\ 0 & 0 & & 0 & -1 \end{pmatrix} \;=\; (-1)^n$$

Here $D_{n+1} = (-1)^n$ is obvious, as it is derived from an upper triangular matrix. And by induction hypothesis we have $D_1 = f_1(t)$ such that the above determinant of $t\mathbb{1}_{n+1} - C$ turns into

$$\det(t\mathbb{1}_{n+1} - C) \;=\; t \cdot f_1(t) + (-1)^{2n+2} a_0 \;=\; t \cdot f_1(t) + a_0 \;=\; f(t)$$

Thus we have completed the induction and found $c_C(t) = f(t)$. It remains to prove, that this also is the minimal polynomial $m_C(t) = f(t)$. However the proof of this needs some more advances in the theory - namely the Cayley-Hamilton theorem and (5.57). However we give the proof here, but abstain from using this property: First of all we have $f(C) = c_C(C) = 0$ by (5.44.(ii)). Let us now denote the endomorphism $\varphi : R^n \to R^n : x \mapsto Cx$. In the Euclidean basis $\mathcal{E}$ of R^n we then have $[\varphi]_\mathcal{E} = C = \mathrm{comp}(f)$. So by (5.57.(iii)) we find the following isomorphism of $R[t]$-modules

$$R[t] \Big/ fR[t] \;\xrightarrow{\sim}\; (R^n)_\varphi \;:\; g + fR[t] \;\mapsto\; ge_1$$

In particular: If $g \in R[t]$ is any polynomial satisfying $g(C) = 0$ then of course $0 = g(C)(e_1) = ge_1$. Due to the injectivety of the map this means $g + fR[t] = 0 + fR[t]$ and hence $f \mid g$. Therefore f satisfies the properties of the minimal polynomial and as this is unique, we have $f = m_C$. □

Proof of (5.44):

(i) Recall the explicit definition of the determinant of a square matrix A, as a sum over all permutations

of n and the respective products

$$\det(A) \;:=\; \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma)\prod_{i=1}^{n} a_{i,\sigma(i)}$$

We will now cluster this sum: For any permutation $\sigma \in S_n$ let us denote the *fixed set* of σ by $\operatorname{fix}(\sigma) := \{\, i \in 1\ldots n \mid \sigma(i) = i \,\}$. Using this we can partition S_n into

$$S_n \;=\; \bigcup_{f=0}^{n} \bigcup_{\substack{F\subseteq 1\ldots n\\ \#F=f}} \{\, \sigma \in S_n \mid \operatorname{fix}(\sigma) = F \,\}$$

For any $i \in F = \operatorname{fix}(\sigma)$ we have $\sigma(i) = i$ by construction. Thus this partition enables us to rewrite the determinant into the form

$$\det(A) \;=\; \sum_{f=0}^{n}\sum_{\#F=f}\sum_{\operatorname{fix}(\sigma)=F} \operatorname{sgn}(\sigma)\prod_{i=1}^{n}\begin{cases} a_{i,i} \text{ if } i \in F \\ a_{i,\sigma(i)} \text{ if } i \notin F \end{cases}$$

If $i \notin F = \operatorname{fix}(\sigma)$ then $a_{i,\sigma(i)}$ is off the diagonal of A, so if we apply this to $\det(t\mathbb{1}_n - A)$ we find the following expression

$$c_A(t) \;=\; \sum_{f=0}^{n}\sum_{\#F=f}\sum_{\operatorname{fix}(\sigma)=F} \operatorname{sgn}(\sigma)\prod_{i=1}^{n}\begin{cases} t - a_{i,i} \text{ if } i \in F \\ -a_{i,\sigma(i)} \text{ if } i \notin F \end{cases}$$

We will prove that this expression can be reformulates as the equality

$$c_A(t) \;=\; \sum_{r=0}^{n}(-1)^{n-r}t^r \sum_{\alpha\in \operatorname{Asc}(n-r,n)} \det\big(A[\alpha \mid \alpha]\big)$$

As R is commutative, the product can be decomposed into two separate parts: Note that the product of the $(t - a_{i,i})$ can be rewritten as a polynomial in t. Thereby the coefficient of t^{f-k} is the elementary symmetric polynomial evaluated in the $a_{i,i}$ where $i \in F \subseteq 1\ldots n$. Let us denote $\operatorname{Asc}(k,F) := \{\, \gamma : 1\ldots k \to F \mid \gamma(1) < \gamma(2) < \cdots < \gamma(k) \,\}$ then these products can be rewritten as

$$\begin{aligned} \prod_{i\notin F}\big(-a_{i,\sigma(i)}\big) &= (-1)^{n-f}\prod_{i\notin F} a_{i,\sigma(i)} \\ \prod_{i\in F}(t - a_{i,i}) &= \sum_{k=0}^{f}(-1)^k t^{f-k} \sum_{\gamma\in\operatorname{Asc}(k,F)}\prod_{j=1}^{k} a_{\gamma(j),\gamma(j)} \end{aligned}$$

Since $\gamma(j) \in F$ for any $j \in 1\ldots k$ we have $\sigma(\gamma(j)) = \gamma(j)$. Thus if we denote $\overline{F} := (1\ldots n) \setminus F$ and $\overline{F} \cup \gamma := \overline{F} \cup \gamma(1\ldots k)$ then combining these two equations we find

$$\prod_{i=1}^{n}\begin{cases} t - a_{i,i} \text{ if } i \in F \\ -a_{i,\sigma(i)} \text{ if } i \notin F \end{cases}$$

$$= \sum_{k=0}^{f} (-1)^{n-f+k} t^{f-k} \sum_{\gamma \in \mathrm{Asc}(k,F)} \prod_{i \in \overline{F} \cup \gamma} a_{i,\sigma(i)}$$

Altogether we can rewrite the characteristic polynomial of A as $c_A(t) =$

$$\sum_{f=0}^{n} \sum_{\#F=f} \sum_{\mathrm{fix}(\sigma)=F} \mathrm{sgn}(\sigma) \sum_{k=0}^{f} (-1)^{n-f+k} t^{f-k} \sum_{\gamma \in \mathrm{Asc}(k,F)} \prod_{i \in \overline{F} \cup \gamma} a_{i,\sigma(i)}$$

We can pull the summation symbol $\sum_k$ in front, right behind $\sum_f$ by the associativity property of the addition, such that the summation runs over all indexes (f,k), where $f, k \in 0 \dots n$ and $k \leq f$. However we can rearrange this index set to the set (r,k), where $r, k \in 0 \dots n$ and $k \leq n-r$. The bijection of these is $(f,k) \mapsto (f-k,k)$ with inverse $(r,k) \mapsto (r+k,k)$. Therefore $c_A(t) =$

$$\sum_{r=0}^{n} (-1)^{n-r} t^r \sum_{k=0}^{n-r} \sum_{\#F=k+r} \sum_{\mathrm{fix}(\sigma)=F} \mathrm{sgn}(\sigma) \sum_{\gamma \in \mathrm{Asc}(k,F)} \prod_{i \in \overline{F} \cup \gamma} a_{i,\sigma(i)}$$

In case $r = n$ we have $k = 0$ and since $\#F = n$ necessarily $F = 1 \dots n$. Thus $\sigma = \mathbb{1}_n$ since this is the only permutation, that fixes the entire set $1 \dots n$. Therefore the case $i \notin F$ is void such that the coefficient of t^n equals 1. In any other case $r < n$ we have to show

$$\begin{aligned} & \sum_{k=0}^{n-r} \sum_{\#F=k+r} \sum_{\mathrm{fix}(\sigma)=F} \mathrm{sgn}(\sigma) \sum_{\gamma \in \mathrm{Asc}(k,F)} \prod_{i \in \overline{F} \cup \gamma} a_{i,\sigma(i)} \\ = & \sum_{\alpha \in \mathrm{Asc}(n-r,n)} \det\big(A[\alpha \mid \alpha]\big) \end{aligned}$$

But this is not too far away: Let us apply the above partition of S_{n-r} to the expression $\det(A[\alpha \mid \alpha])$, then we have the equality

$$\begin{aligned} & \sum_{\alpha \in \mathrm{Asc}(n-r,n)} \det\big(A[\alpha \mid \alpha]\big) \\ = & \sum_{\alpha \in \mathrm{Asc}(n-r,n)} \sum_{f=0}^{n-r} \sum_{\#F=f} \sum_{\mathrm{fix}(\varrho)=F} \mathrm{sgn}(\varrho) \prod_{i=1}^{n-r} \begin{cases} a_{\alpha(i),\alpha(i)} & \text{if } i \in F \\ a_{\alpha(i),\alpha\varrho(i)} & \text{if } i \notin F \end{cases} \end{aligned}$$

Rearranging a little we can pull out the summation symbol $\sum_f$ up front and push the summation $\sum_\alpha$ behind $\mathrm{sgn}(\varrho)$. Then we see that both expressions start with a summation from 0 to $n-r$. Thus if we take the same summation index $f = k$ it suffices to show the equality of

$$\begin{aligned} & \sum_{\#F=k+r} \sum_{\mathrm{fix}(\sigma)=F} \mathrm{sgn}(\sigma) \sum_{\gamma \in \mathrm{Asc}(k,F)} \prod_{i \in \overline{F} \cup \gamma} a_{i,\sigma(i)} \\ = & \sum_{\#F=f} \sum_{\mathrm{fix}(\varrho)=F} \mathrm{sgn}(\varrho) \sum_{\alpha \in \mathrm{Asc}(n-r,n)} \prod_{i=1}^{n-r} \begin{cases} a_{\alpha(i),\alpha(i)} & \text{if } i \in F \\ a_{\alpha(i),\alpha\varrho(i)} & \text{if } i \notin F \end{cases} \end{aligned}$$

Note that in these terms both products encompass $n-r$ entries of A. For $\det(A[\alpha \mid \alpha])$ this is obvious and for $c_A(t)$ note that $\#F = k+r$ such that $\#\overline{F} = n-k-k$ and as $\#\gamma(1 \dots k) = k$ and $\gamma(1 \dots k) \subseteq F$ this means $\#(\overline{F} \cap \gamma) = n-k+r+k = n-r$. Let us take a closer look at these

products

$$\prod_{i=1}^{n-r}\begin{cases} a_{\alpha(i),\alpha(i)} \text{ if } i \in F \\ a_{\alpha(i),\alpha\varrho(i)} \text{ if } i \notin F \end{cases} = \prod_{i\in F} a_{\alpha(i),\alpha(i)} \prod_{i\notin F} a_{\alpha(i),\alpha\varrho(i)}$$
$$\prod_{i\in\overline{F}\cup\gamma} a_{i,\sigma(i)} = \prod_{j\in\gamma(1\ldots k)} a_{j,j} \prod_{j\notin F} a_{j,\sigma(j)}$$

We are being a little sloppy, as in the upper term $F \subseteq I := 1\ldots(n-r)$ differs from $F \subseteq J := 1\ldots n$ in the lower term. Let us rename these sets F_I and F_J respectively. Then $\alpha : I \hookrightarrow J$ and $\varrho \in S_I$ such that we may consider $\sigma := \alpha\varrho\alpha^{-1}$. We can regard $\sigma \in S_I$ if we take $\sigma(j) := j$ for any $j \in 1\ldots n \setminus \alpha(I)$. With this continuation we find

$$\mathrm{fix}(\sigma) = \alpha(\mathrm{fix}(\varrho))\overline{\alpha(I)}$$

Prob If $j \notin \alpha(I)$ then $j \in \mathrm{fix}(\sigma)$ by construction and if $j = \alpha(i)$ then $j = \sigma(j) = \alpha\varrho\alpha^{-1}(j)$ if and only if $\alpha^{-1}(j) = \varrho\alpha^{-1}(j)$ which is $i = \varrho(i)$ or in other words $i \in \mathrm{fix}(\varrho)$ such that $j \in \alpha(\mathrm{fix}(\varrho))$.

Altogether, if we use the bijection $F_I \mapsto F_J := \alpha(F_I) \cup \overline{\alpha(I)}$ we turn the subset $F_I \subseteq 1\ldots(n-r)$ with f elements into a subset $F_J \subseteq 1\ldots n$ with $f+r$ elements. And if $F_I = \mathrm{fix}(\varrho)$ then for $\varrho \mapsto \sigma = \alpha\varrho\alpha^{-1}$ we find $\mathrm{fix}(\sigma) = F_J$. Thereby it is clear that $\mathrm{sgn}(\sigma) = \mathrm{sgn}(\varrho)$ as conjugation does not change the cyclic structure of ϱ. All we have to do is define $\gamma \in \mathrm{Asc}(k, F_J)$ to be the one ascending chain of indexes with $\gamma(1\ldots k) = \alpha(F_I)$. As F_I has $f = k$ elements and $\alpha(F_I) \subseteq F_J$, this is well defined. Thus we have translated the lower term into the upper term using $F_I \mapsto F_J$, $\varrho \mapsto \sigma$ and $\alpha \mapsto \gamma$. But from this construction it is clear that the products match each other

$$\prod_{j\in\gamma(1\ldots k)} a_{j,j} = \prod_{i\in F_I} a_{\alpha(i),\alpha(i)}$$
$$\prod_{j\notin F_J} a_{j,\sigma(j)} = \prod_{i\notin F_I} a_{\alpha(i),\alpha\varrho(i)}$$

(ii) Let $B := (t\mathbb{1}_n - A)^{\#} \in \mathrm{mat}_n(R[t])$ be the adjugate matrix of $t\mathbb{1}_n - A$, then (as $R[t]$ is a commutative ring) we have seen in (4.63.(iii)) that

$$(t\mathbb{1}_n - A)B = \det(t\mathbb{1}_n - A)\mathbb{1}_n = c_A(t)\mathbb{1}_n$$

That is we have n^2 equations in the polynomial ring $R[t]$ encoded in a single equation for $n \times n$ matrices over $R[t]$. And by construction the degree of all these polynomial equations is n. Let us now write

$$B = (t\mathbb{1}_n - A)^{\#} = \sum_{k=0}^{n-1} t^k B_k$$

for sufficient $B_k \in \mathrm{mat}_n(R)$, then the above equation takes the form

$$c_A(t)\mathbb{1}_n = (t\mathbb{1}_n - A)\sum_{k=0}^{n-1} t^k B_k = \sum_{k=0}^{n-1} t^{k+1} B_k - \sum_{k=0}^{n-1} t^k A B_k$$
$$= t^n B_{n-1} + \sum_{k=1}^{n-1} t^k (B_{k-1} - AB_k) - AB_0$$

Comparing coefficients yields $c_A[n]\mathbb{1}_n = B_{n-1}$ and hence $B_{n-1} = \mathbb{1}_n$ as $c_A(t)$ is monic: $c_A[n] = 1$. Also $AB_0 = -c_A[0]\mathbb{1}_n = -(-1)^n \det(A)\mathbb{1}_n$. Also this is no wonder, as $B_0 = -A^\#$. Also for any $k \in 1 \ldots (n-1)$

$$c_A[k]\mathbb{1}_k \;=\; B_{k-1} - AB_k$$

Let us now multiply all these equations with A^k from the left, that is $B_{n-1}A^n = A^n$ and for any $k \in 1 \ldots n-1$ we get

$$c_A[k]A^k \;=\; A^k B_{k-1} - A^{k+1}B_k$$

Then $c_A(A) = \sum_k c_A[k]A^k$ can be replaced in every coefficient $c_A[k]A^k$ separately to find a telescopic sum, that vanishes identically

$$\begin{aligned}
c_A(A) &= \sum_{k=0}^{n} c_A[k]A^k \;=\; A^n + \sum_{k=1}^{n-1} c_A[k]A^k + c_A[0]\mathbb{1}_n \\
&= A^n + \sum_{k=1}^{n-1} (A^k B_{k-1} - A^{k+1}B_k) + c_A[0]\mathbb{1}_n \\
&= A^n + \sum_{k=1}^{n-1} A^k B_{k-1} - \sum_{k=2}^{n} A^k B_{k-1} + c_A[0]\mathbb{1}_n \\
&= A^n + AB_0 - A^n B_{n-1} + c_A[0]\mathbb{1}_n \\
&= A^n - c_A[0]A - A^n + c_A[0]\mathbb{1}_n \;=\; 0
\end{aligned}$$

(iii) Pick up an ordered basis $\mathcal{M}$ of M and let $A := [\varphi]_{\mathcal{M}}$ be the matrix representation of $\varphi \in \mathrm{end}(M)$. Then the characteristic polynomial of φ has been defined, as $c_\varphi(t) = c_A(t) \in R[t]$. As $\varphi \mapsto [\varphi]_{\mathcal{M}}$ is an isomorphism of R-algebras, according to (4.40), we find

$$\big[c_\varphi(\varphi)\big]_{\mathcal{M}} \;=\; c_\varphi\left([\varphi]_{\mathcal{M}}\right) \;=\; c_\varphi(A) \;=\; c_A(A) \;=\; 0$$

as we have just seen in (ii). Therefore $c_\varphi(\varphi) = 0 \in \mathrm{end}(M)$ is the zero-map, which had to be proved.

(iv) As M is finitely generated we find some $x_k \in M$ such that $M = \mathrm{Lh}\{\, x_1, \ldots, x_n \,\}$ where $n = \mathrm{rank}(M)$. Now, as $\varphi(x_j) \in M$ again, for any $j \in 1 \ldots n$ we also find some $a_{i,j} \in R$ such that

$$\varphi(x_j) \;=\; \sum_{i=1}^{n} a_{i,j} x_i$$

Let $A := (a_{i,j}) \in \mathrm{mat}_n(R)$ be the $n \times n$ matrix of those coefficients. Then it is clear that for any $x = \sum_j b_j x_j \in M$ we get

$$\begin{aligned}
\varphi(x) &= \sum_{j=1}^{n} b_j \varphi(x_j) \;=\; \sum_{j=1}^{n} b_j \sum_{i=1}^{n} a_{i,j} x_i \\
&= \sum_{i=1}^{n} \left(\sum_{i=1}^{n} a_{i,j} b_j \right) x_i \;=\; \sum_{i=1}^{n} [Ab]_i \, x_i
\end{aligned}$$

where we denoted $b = (b_1, \ldots, b_n) \in R^n$ the coefficient-vector of x. And likewise $\varphi^k(x) =$

$\sum_i [A^k b]_i \, x_i$. Now let $f(t) := \det(t\mathbb{1}_n - A)$ be the characteristic polynomial of A again. Then we have shown in (i) that $f(A) = 0$. And hence for any $x = \sum_j b_j \in M$ we find

$$\begin{aligned} c(\varphi)(x) &= \sum_{k=0}^{n} f[k]\varphi^k(x) = \sum_{k=0}^{n} f[k] \sum_{i=1}^{n} [A^k b]_i \, x_i \\ &= \sum_{i=1}^{n} \left(\sum_{k=0}^{n} f[k][A^k b]_i \right) x_i = \sum_{i=1}^{n} \left[\sum_{k=0}^{n} f[k] A^k b \right]_i x_i \\ &= \sum_{i=1}^{n} [f(A)b]_i \, x_i = \sum_{i=1}^{n} 0 \, x_i = 0 \end{aligned}$$

(v) Let $\{ m_1, \ldots, m_n \}$ be a generating set of M as an R-module. Then by assumption $\varphi(m_i) \in \varphi(M) \subseteq \mathfrak{a}M$ and therefore by (3.40.(ii)) there are some elements $a_{i,j} \in \mathfrak{a}$ such that

$$\varphi(m_i) = \sum_{j=1}^{n} a_{i,j} m_j$$

Let $A := (a_{i,j}) \in \mathrm{mat}_n(R)$ be the $(n \times n)$-matrix of these coefficients $c_A \in R[t]$ be the characteristic polynomial of A. By (i) we have $c_A[0] = \pm\det(A)$ which is an n-fold product of the elements $a_{i,j}$. In particular $c_A[0] \in \mathfrak{a}$ [even $c_A[0] \in \mathfrak{a}^n$]. Likewise $c_A[n-1] = -\mathrm{tr}(A)$ and hence $c_A[n-1] \in \mathfrak{a}$ as well. Generally $c_A[k] \in \mathfrak{a}$ [even $c_A[k] \in \mathfrak{a}^{n-k}$] is clear, by the general formula in (i).

Let $R[\varphi] = \{ f(\varphi) \mid f \in R[t] \}$ be the sub-ring of $\mathrm{end}(M)$ generated by φ and note that this is a commutative ring. Then the above equations can be reformulated - for any $i \in 1 \ldots n$ - into

$$\sum_{j=1}^{n} (\delta_{i,j}\varphi - a_{i,j}\mathbb{1}) m_j = 0$$

Thus, if we regard the $(n \times n)$-matrix $\Phi := (\delta_{i,j}\varphi - a_{i,j}\mathbb{1}) \in \mathrm{mat}_n(R[\varphi])$ then we find that $\Phi(m_1, \ldots, m_n) = (0, \ldots, 0) \in M^n$. In particular by (4.63.(iii)) we have

$$\det(\Phi) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \Phi^{\#}\Phi \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \Phi^{\#} \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

That is $\det(\Phi) \in R[\varphi]$ annihilates any $m_i \in M$ and therefore $\det(\Phi) = 0 \in \mathrm{end}(M)$. But oviously $\det(\Phi) = c_A(\varphi)$ and as we have argued above $c_A(t) \in R[t]$ is a polynomial of the required form.

□

Proof of (3.44):

(i) Let us denote $J := \{ i \in I \mid m_i \notin \mathfrak{a}M \}$, then we have to prove that $\{ m_j + \mathfrak{a}M \mid j \in J \}$ is an $(R/\mathfrak{a})$-basis of $M/\mathfrak{a}M$. So we first have to check, that this set $(R/\mathfrak{a})$-linearly generates $M/\mathfrak{a}M$. Thus consider any $x + \mathfrak{a}M \in M/\mathfrak{a}M$, that is $x \in M$. As the m_i generate M there are some $a_i \in R$ (where $i \in I$ and only finitely many $a_i \neq 0$ are non-zero), such that $x = \sum_i a_i m_i$. And thereby we

already get

$$\begin{aligned} x + \mathfrak{a}M &= \sum_{i\in I} a_i m_i + \mathfrak{a}M = \sum_{i\in I} (a_i + \mathfrak{a})(m_i + \mathfrak{a}M) \\ &= \sum_{i\in J} (a_i + \mathfrak{a})(m_i + \mathfrak{a}M) \end{aligned}$$

where the latter equality holds, as any $i \in I \setminus J$ yields $x_i + \mathfrak{a}M = 0 + \mathfrak{a}M$. It remains to prove the $(R/\mathfrak{a})$-linear independence of this set. Thus suppose we are given any $b_j + \mathfrak{a} \in R/\mathfrak{a}$ (of which only finitely many are non-zero) such that

$$0 + \mathfrak{a}M = \sum_{j\in J} (b_j + \mathfrak{a})(m_j + \mathfrak{a}M) = \sum_{j\in J} b_j m_j + \mathfrak{a}M$$

In other terms that is $\sum_j b_j m_j \in \mathfrak{a}M$. But as $\{ m_i \mid i \in I \}$ generates M we may use (3.40.(ii)) to find some $a_i \in \mathfrak{a}$, of which only finitely many are non-zero, such that

$$\sum_{j\in J} b_j m_j = \sum_{i\in I} a_i m_i$$

As the m_i form an R-basis of M we may compare coefficients in these two representations, which yields $a_i = 0$ for any $i \in I \setminus J$ and $b_j = a_j \in \mathfrak{a}$ for any $j \in J$. Hence we have $b_j + \mathfrak{a} = 0$ for any $j \in J$ and this is the $(R/\mathfrak{a})$-linear independence of $\{ m_j + \mathfrak{a}M \mid j \in J \}$.

(i) It remains to prove that the $m_i + \mathfrak{a}M$ are pairwise distinct, too. First, if $\mathfrak{a} = R$, then $\mathfrak{a}M = M$ and hence $m_i \in \mathfrak{a}M$ for any $i \in I$. In this case the basis given is empty and there is nothing to prove. So let us now assume $\mathfrak{a} \neq 0$. If $m_i + \mathfrak{a}M = m_j + \mathfrak{a}M$ then we have $m_i - m_j \in \mathfrak{a}M$. Yet as $\{ m_i \mid i \in I \}$ generates M we may use (3.40.(ii)) again, to find some $a_k \in \mathfrak{a}$, of which only finitely many are non-zero, such that

$$m_i - m_j = \sum_{k\in I} a_k m_k$$

If we had $i \neq j$ then this would yield an equation of R-linear dependence, simply by moving $m_i - m_j$ on the left hand side and decomposing

$$(a_i - 1)m_i + (a_j + 1)m_j + \sum_{\substack{k\in I,\\ k\neq i,j}} a_k m_k = 0$$

As the m_i are R-linearly independent this implies all coefficients in this equation to be 0, in particular $1 = a_i \in \mathfrak{a}$. That is $\mathfrak{a} = R$ which cannot occur. Hence we necesserily have $i = j$.

(ii) (a) $\implies$ (b): let us choose a generating set $\{ m_1, \ldots, m_n \}$ of M with a minimal number n of elements. Suppose $n \geq 1$ then, as $m_1 \in M = \mathfrak{a}M$ we may invoke (3.40.(ii)) to find some $a_1, \ldots, a_n \in \mathfrak{a}$ such that $m_1 = a_1 m_1 + \cdots + a_n m_n$. Let us now write this equation in the form

$$(1 - a_1)m_1 = a_2 m_2 + \cdots + a_n m_n$$

As $a_1 \in \mathfrak{a} \in \operatorname{JAC}(R)$ we know by (2.8) that $1 - a_1 \in R^*$ is invertible. And hence m_1 is contained in

the linear hull of $\{ m_2, \ldots, m_n \}$ by

$$m_1 \;=\; \sum_{i=2}^{n} (1-a_1)^{-1} a_i \, m_i$$

That is even $\{ m_2, \ldots, m_n \}$ generates M in contradiction to the minimality of the number n of generators. So our assumption $n \geq 1$ has been false, that is $n = 0$ and hence $M = 0$.

$\neg$ (a) $\Longrightarrow$ $\neg$ (b): if $\mathfrak{a} \not\subseteq \operatorname{JAC}(R)$ then - by definition of the Jacobson radical - there is a maximal ideal $\mathfrak{m} \trianglelefteq_{\mathfrak{i}} R$ of R such that $\mathfrak{a} \not\subseteq \mathfrak{m}$. And this again means that there is some $u \in \mathfrak{a}$ with $u \notin \mathfrak{m}$. Now, as $M := R/\mathfrak{m}$ is a field, and $u + \mathfrak{m} \neq 0 \in M$ there is some $v + \mathfrak{m} \in M$ such that $uv + \mathfrak{m} = (u + \mathfrak{m})(v + \mathfrak{m}) = 1 + \mathfrak{m}$. Clearly M also is finitely generated, by $\{ 1 + \mathfrak{m} \}$ as an R-module. Also

$$\begin{aligned} \mathfrak{a}M &= \{ ab + \mathfrak{m} \mid a \in \mathfrak{a},\ b \in R \} \\ &= \{ c + \mathfrak{m} \mid c \in R \} \;=\; M \end{aligned}$$

Hereby the central equality is due to the following reasoning: given $c \in R$ we may take $a := u$ and $b := vc$, that $ab + \mathfrak{m} = uvc + \mathfrak{m} = c + \mathfrak{m}$, and the converse inclusion is clear. Thus we have found a finitely generated R-module M with $\mathfrak{a}M = M$, but $M \neq 0$.

(ii) **Alternative Version:** the more advanced lemma of Dedekind allows to prove the implication (a) $\Longrightarrow$ (b) in a straightforward way: as M is finitely generated we find some $a \in \mathfrak{a}$ such that $(1-a)M = 0$, due to (v). Yet as $a \in \mathfrak{a} \subseteq \operatorname{JAC}(R)$ proposition (2.8) yields that $1 - a \in R^*$ is invertible. Hence $M = (1-a)M = 0$ is proved already.

(iii) By (3.40.(v)) we have know that $\mathfrak{a}(M/P)$ equals $(\mathfrak{a}M + P)/P$ and hence we have the following identities (by the assumptions on P)

$$\mathfrak{a}\left(M \Big/ P \right) \;=\; \mathfrak{a}M + P \Big/ P \;=\; M \Big/ P$$

Yet M/P is finitely generated and $\mathfrak{a} \subseteq \operatorname{JAC}(R)$ so by the lemma of Nakayama (ii) we get $M/P = 0$ and this is nothing but $M = P$.

(iv) If φ is surjective, then $\varphi/\mathfrak{a}$ clearly is surjective as well - see (3.40.(vi)) for details. So conversely assume $\varphi/\mathfrak{a}$ is surjective, that is for any $y \in N$ there is some $x \in M$ that

$$y + \mathfrak{a}N \;=\; \varphi \Big/ \mathfrak{a}(x + \mathfrak{a}M) \;=\; \varphi(x) + \mathfrak{a}N$$

That is $v := y - \varphi(x) \in \mathfrak{a}N$, such that $y = \varphi(x) + v$. As y has been arbitrary this means $N = \operatorname{im}(\varphi) + \mathfrak{a}N$. Yet as $N/\operatorname{im}(\varphi)$ is finitely generated and $\mathfrak{a} \subseteq \operatorname{JAC}(R)$ this implies $\operatorname{im}(\varphi) = N$ by (iii), which is nothing, but the surjectivity of φ.

(v) ($\diamondsuit$) If φ is bijective, then $\varphi/\mathfrak{m}$ is bijective for any ideal $\mathfrak{a} \subseteq R$, as we have seen in (3.40.(vii)). Conversely: as M is finitely generated, the zero-module $0 \leq_{\mathfrak{m}} M$ is cofinite and hence also $\operatorname{im}(\varphi) \leq_{\mathfrak{m}} M$ is cofinite. So by (iv) we already know, that φ is surjective, as $\varphi/\mathfrak{a}$ is surjective (even bijective). But a surjective endomorphism of a finitely generated R-module already is bijective by (5.44).

(vi) ($\diamondsuit$) Consider the identity-map $\mathbb{1} : M \to M : x \mapsto x$ on M. Clearly this is an R-linear map satisfying $\mathrm{im}(\mathbb{1}) \subseteq M = \mathfrak{a}M$. And as M is finitely generated the Cayley-Hamilton theorem (5.44) yields some polynomial $f = t^n + a_1 t^{n-1} + \cdots + a_n \in R[t]$ such that $f(\mathbb{1}) = 0$ and $a_k \in \mathfrak{a}^k$ for any $k \in 1 \ldots n$. Now compute

$$\begin{aligned} f(\mathbb{1}) &= \mathbb{1}^n + a_1\mathbb{1}^{n-1} + \cdots + a_{n-1}\mathbb{1} + a_n\mathbb{1} \\ &= (1 + a_1 + \cdots + a_n)\mathbb{1} \;=\; (1-a)\mathbb{1} \end{aligned}$$

where we let $a := -(a_1 \cdots + a_n) \in \mathfrak{a}$. Now $0 = \mathrm{im}(0) = \mathrm{im}(f(\mathbb{1})) = \mathrm{im}((1-a)\mathbb{1}) = (1-a)M$. That is the $a \in \mathfrak{a}$ we constructed using Cayley-Hamilton truly satisfies $(1-a)M = 0$.

□

Proof of (3.82):

(iii) In case of a skew-field S things are simple now: according to the dimension formula (3.68.(iii)) we know that

$$\dim(V) \;=\; \dim(\mathrm{kn}(\varphi)) + \dim(\mathrm{im}(\varphi))$$

This if φ is injective then we have $\mathrm{kn}(\varphi) = 0$ and hence $\dim(\mathrm{kn}(\varphi)) = 0$ which leaves $\dim(V) = \dim(\mathrm{im}(\varphi))$. Thus (as V is finite dimensional) by (3.64.(ix)) we find that $\mathrm{im}(\varphi) = V$ such that φ is surjective.

Conversely if φ is surjective, then $\mathrm{im}(\varphi) = V$ and hence $\dim(\mathrm{im}(\varphi)) = \dim(V)$, which leaves $\dim(\mathrm{kn}(\varphi) = 0$. Therefore $\mathrm{kn}(\varphi) = 0$ [if there was some $0 \neq x \in \mathrm{kn}(\varphi)$, then $\{ x \}$ would be a linearly independent set in $\mathrm{kn}(\varphi)$ and hence $\dim(\mathrm{kn}(\pi)) \geq 1$]. But of course this means that φ is injective.

So in any case we have seen surjective implies bijective and injective implies bijective. And the converse implications are trivial.

(ii) Any power of φ is an endomorphism again, so let us consider the following descending chain of sumbodules of M

$$\mathrm{im}(\varphi) \;\supseteq\; \mathrm{im}(\varphi^2) \;\supseteq\; \ldots \;\supseteq\; \mathrm{im}(\varphi^n) \;\supseteq\; \mathrm{im}(\varphi^{n+1}) \;\supseteq\; \ldots$$

As M is artinian this chain has to stabilize, that is there is some $n \in \mathbb{N}$ such that $\mathrm{im}(\varphi^n) = \mathrm{im}(\varphi^{n+1}) = \ldots$. Let us denote $\psi := \varphi^n$. Then $\psi : M \to M$ still is injective and if we denote $P := \mathrm{im}(\psi)$, then trivially $\psi : M \to P$ is surjective and hence an isomorphism of modules. Yet we also get

$$P \;=\; \mathrm{im}(\psi) \;=\; \mathrm{im}(\varphi^n) \;=\; \mathrm{im}(\varphi^{2n}) \;=\; \mathrm{im}(\psi^2) \;=\; \psi^2(M) \;=\; \psi(P)$$

From $\psi(P) = P$ we also find, that $\psi : P \xrightarrow{\sim} P$ is an automorphism on P. Now consider any $x \in M$ and let $y := \psi(x) \in P$. As $\psi : P \xrightarrow{\sim} P$ we find that $x = \psi^{-1}(y) \in P$. Hence $M \subseteq P \subseteq M$ such that $\psi : M \xrightarrow{\sim} M$ is an automorphism on M. Thus φ must have been bijective already, the inverse is given to be $\varphi^{n-1}\psi^{-1}$.

(i) **Dedekind-Proof**: We will first present a rather short proof using the lemma of Dedekind: Let us regard M as an $R[t]$-module by virtue of (5.53). Then by construction we get $tx = \varphi(x)$ for any

$x \in M$ hence, as φ is surjective, for any $y \in M$ there is some $x \in M$ with $tx = y$. Hence we get $tM = M$, in particular $\mathfrak{a}M = M$ for $\mathfrak{a} := tR[t] \trianglelefteq_{\mathfrak{i}} R[t]$. Now by then lemma of Dedekind (3.44.(vi)) there is some $g \in \mathfrak{a}$ such that $(1-g)M = 0$. As $g \in \mathfrak{a}$ there is some $f \in R[t]$ with $g(t) = tf(t)$. Let us define $\psi := g(\varphi) \in \mathrm{end}(M)$. Then $gx = g(\varphi)(x) = \psi(x)$ for any $x \in M$ and hence $(1-f)M = 0$ implies

$$0 \;=\; (1 - tg(t))x \;=\; x - t\psi(x) \;=\; x - \varphi(\psi(x))$$

$$0 \;=\; (1 - gt(t))x \;=\; x - g\varphi(x) \;=\; x - \psi(\varphi(x))$$

That is $\varphi(\psi(x)) = x$ and $\psi(\varphi(x)) = x$ for any $x \in M$. That is ψ is just the inverse map of φ and in particular φ is bijective.

(i) **Noether-Proof**: As the proof above requires the somewhat abstract Dedekind lemma, we would like to supply another proof that requires the theory of noetherian modules only. As M is finitely generated there are some $x_i \in M$ such that $M = \mathrm{Lh}(x_1, \ldots, x_n)$. Then, as $\varphi(x_j) \in M$ we can pick up some $p_{i,j} \in R$ such that

$$\varphi(x_j) \;=\; \sum_{i=1}^{n} p_{i,j} x_i$$

Step (A): we will now prove, that $M = \mathrm{Lh}(\varphi(x_1), \ldots, \varphi(x_n))$. That is we choose some $y \in M$ arbitarily. As φ is surjective there is some $x \in M$ such that $y = \varphi(x)$. And hence there are some $a_j \in R$ such that $x = \sum_j a_j x_j$. Now compute

$$y \;=\; \varphi(x) \;=\; \sum_{j=1}^{n} a_j \varphi(x_j) \;\in\; \mathrm{Lh}\Big(\varphi(x_1), \ldots, \varphi(x_n)\Big)$$

Step (B): as the $\varphi(x_j)$ generate M we can conversely choose some $q_{j,i} \in R$ such that the $x_i \in M$ can be written as

$$x_i \;=\; \sum_{j=1}^{n} q_{j,i} \varphi(x_j)$$

Remember all we have to prove is the injectivity of φ. And to do this it suffices to prove $\mathrm{kn}(\varphi) = 0$. Hence regard some $k \in M$ with $\varphi(k) = 0$. All we have to prove is $k = 0$, then the injectivity is established.

Step (C): write k as $k = \sum_i k_i x_i$ for some $k_i \in R$ and let A denote the $\mathbb{Z}$-algebra generated by all the $p_{i,j}$ $q_{i,j}$ and k_i

$$A \;:=\; \mathbb{Z}\left[\bigcup_{i=1}^{n}\bigcup_{j=1}^{n} \{\, p_{i,j}, q_{i,j}, k_i \,\}\right]$$

Then A is finitely generated and $\mathbb{Z}$ is notherian (even a PID) such that A is a noetherian sub-ring of R, by the Hilbert basis theorem (2.42). Also let N be the A-sub-module of M that is generated by the x_i. As N is a finitely generated module over the noetherian ring N is a noetherian A-module itself

$$N \;:=\; \mathrm{Lh}_A(x_1, \ldots, x_n)$$

Step (D): we will now prove that $\varphi : N \to M$ restricts to $\varphi : N \to N$. That is we will prove that

$\varphi(x) \in N$ for any $x \in N$. But this is easy to see: if $x \in N$ then $x = \sum_j a_j x_j$ for some $a_j \in N$. Hence

$$\varphi(x) \;=\; \sum_{j=1}^{n} a_j \varphi(x_j) \;=\; \sum_{j=1}^{n} a_j \sum_{i=1}^{n} p_{i,j} x_i \;=\; \sum_{i=1}^{n} \sum_{j=1}^{n} p_{i,j} a_j x_i$$

and this is contained in N again, as $p_{i,j} \in A$ as well. Also we will prove that $\varphi : N \twoheadrightarrow N$ is surjective, that is for any $y \in N$ there is some $x \in N$ such that $y = \varphi(x)$. If $y = \sum_i b_i x_i$ then let $x := \sum_i b_i \sum_j q_{i,j} \in A$

$$\varphi(x) \;=\; \sum_{i=1}^{n} b_i \sum_{j=1}^{n} q_{i,j} \varphi(x_j) \;=\; \sum_{i=1}^{n} b_i x_i \;=\; y$$

Step (E): as $\varphi : N \to N$ is surjective, so is $\varphi^k : N \to N$. Now let $K_i := \mathsf{kn}(\varphi^k) \;\leq_{\mathsf{m}}\; N$. Then it is clear, that the K_i form an ascending chain of sub-modules of N

$$K_0 \;\subseteq\; K_1 \;\subseteq\; K_2 \;\subseteq\; \ldots$$

But as N is noetherian this chain has to stabilize, that is there is some $s \in \mathbb{N}$ such that $K_{s+1} = K_s$. As φ^s is surjective and $k \in N$, there is some $z \in N$ such that $k = \varphi^s(z)$. But now $0 = \varphi(k) = \varphi(\varphi^s(z)) = \varphi^{s+1}(z)$ implies $z \in K_{s+1} = K_s$. That is $k = \varphi^s(z) = 0$ already. Hence we have finally arrived at $k = 0$ which is the injectivity of $\varphi : M \to M$.

□

Proof of (5.53):
It is clear that $(M_\varphi, +)$ is a commutative group, as we did neither change the base set $M_\varphi = M$ nor the addition $+$ on M. It remains to prove the properties (M) of an $R[t]$-module. Thus consider any f, $g \in R[t]$ and any x, $y \in M$. As φ is R-linear so are the compositions φ^k and hence we can compute

$$\begin{aligned}
1x &= t^0 x \;=\; \varphi^0(x) \;=\; \mathbb{1}_M(x) \;=\; x \\
f(x+y) &= \sum_{k=0}^{\infty} f[k]\varphi^k(x+y) \;=\; \sum_{k=0}^{\infty} f[k]\left(\varphi^k(x) + \varphi^k(y)\right) \\
&= \sum_{k=0}^{\infty} f[k]\varphi^k(x) + \sum_{k=0}^{\infty} f[k]\varphi^k(y) \;=\; fx + fy \\
(f+g)x &= \sum_{k=0}^{\infty} (f[k] + g[k])\varphi^k(x) \\
&= \sum_{k=0}^{\infty} f[k]\varphi^k(x) + \sum_{k=0}^{\infty} g[k]\varphi^k(x) \;=\; fx + gx \\
f(gx) &= \sum_{i=0}^{\infty} f[i]\varphi^i\left(\sum_{j=0}^{\infty} g[j]\varphi^j(x)\right) \\
&= \sum_{i=0}^{\infty} f[i] \sum_{j=0}^{\infty} g[j]\varphi^i\left(\varphi^j(x)\right) \\
&= \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} f[i]g[j]\varphi^{i+j}(x) \\
&= \sum_{k=0}^{\infty} \left(\sum_{i+j=k} f[i]g[j]\right)\varphi^k(x) \;=\; (fg)x
\end{aligned}$$

□

Proof of (5.55):

(i) First of all the additive structures of M and M_μ are just the same, so whether P is a sub-module $P \leq_{\mathsf{m}} M$ resp. $P \leq_{\mathsf{m}} M_\mu$ depends on whether it is closed under scalar multiplications only. Yet, if $a \in R$ and $x \in M$ then we have

$$(at^0)x \;=\; a\mathbb{1}_M(x) \;=\; ax$$

regardless of μ. So if P is a sub-module of M_μ then it already is a sub-module of M. Also note, that for any $x \in P$ we then get

$$\mu(x) \;=\; tx \;\in\; P$$

such that $\mu(P) \subseteq P$ for any $P \leq_{\mathsf{m}} M_\mu$. And if conversely $P \leq_{\mathsf{m}} M$ with $\mu(P) \subseteq P$, then by induction it is clear, that $\mu^k(P) \subseteq P$ for any $k \in \mathbb{N}$. But then we find $fx \in P$ for any $f \in R[t]$ and $x \in P$, since

$$\left(\sum_{k=0}^{n} a_k t^k\right) x \;=\; \sum_{k=0}^{n} a_k \mu^k(x) \;\in\; P$$

That is such a P is closed under scalar multiplications of $R[t]$ (and closed under addition from the start) such that $P \leq_{\mathsf{m}} M_\mu$.

(ii) As the additive structures of M and M_μ resp. of N and N_ν are just the same the $R[t]$-linearity of $\varphi : M_\mu \to N_\nu$ only depends on whether it respects the scalar multiplication. As $(at^0)x = ax$ again, we see that any $R[t]$-linear map $\varphi : M_\mu \to N_\nu$ already is R-linear, as well, since $\varphi(ax) = \varphi((at^0)x) = (at^0)\varphi(x) = a\varphi(x)$. Also note

$$\varphi\big(\mu(x)\big) \;=\; \varphi(tx) \;=\; t\varphi(x) \;=\; \nu\big(\varphi(x)\big)$$

So the $R[t]$-linearity also implies the commutativity $\varphi\mu = \nu\varphi$. Conversely if $\varphi : M \to N$ is R-linear and commutes with μ and ν then by induction it is clear that $\varphi\mu^k = \nu^k\varphi$ for any $k \in \mathbb{N}$ [with $k = 0$ being the R-liearity itself]. And this yields the $R[t]$-linearity of φ

$$\begin{aligned}\varphi\left(\left(\sum_{k=0}^{n} a_k t^k\right) x\right) \;&=\; \varphi\left(\sum_{k=0}^{n} a_k \mu^k(x)\right) \;=\; \sum_{k=0}^{n} a_k \varphi\left(\mu^k(x)\right)\\ &=\; \sum_{k=0}^{n} a_k \nu^k\left(\varphi(x)\right) \;=\; \left(\sum_{k=0}^{n} a_k t^k\right)\varphi(x)\end{aligned}$$

(iii) If $\Phi : M_\mu \xrightarrow{\sim} M_\varepsilon$ is an isomorphism, then by (ii) we already know that $\Phi : M \to M$ is a homomorphism with $\Phi\mu = \varepsilon\Phi$. But as Φ is bijective $\Phi : M \to M$ is an automorphism and we find $\Phi\mu\Phi^{-1} = \varepsilon$ by applying Φ^{-1} from the right. Conversely if $\Phi : M \xrightarrow{\sim} M$ is an automorphism with $\varepsilon = \Phi\mu\Phi^{-1}$ then equivalently $\Phi\mu = \varepsilon\Phi$ such that by (ii) again $\Phi : M_\mu \to M_\varepsilon$ is a homomorphism. But as Φ is bijective, this even is an isomorphism of these modules.

□

Proof of (5.56):

(i) Consider any fx, $gx \in R[t]$, then $fx + gx = (f+g)x$ and as $f+g \in R[t]$ this means $fx+gx \in R[t]$. Also for any $a \in R[t]$ we have $a(fx) = (af)x$ again, by (5.53). And as $af \in R[t]$ this means, that we also have $a(fx) \in R[t]$. In particular, for any $a \in R$, $ax = (a\mathbf{1})x \in R[t]$ such that $Rx \subseteq R[t]x$. It remains to prove, that $R[t]x$ is φ-invariant. Yet by definition of the scalar multiplication on M_φ we have $\varphi(fx) = t(fx) = (tf)x \in R[t]x$ again.

(i) Let us now prove the explicit description of $R[t]x$: Clearly $\varphi^k(x) = t^k x \in R[t]x$, such that the linear hull of the $\varphi^k(x)$ is contained in $R[t]x$. Conversely consider any $fx \in R[t]x$, that is $f \in R[t]$. Let $n := \deg(f)$, then we find that fx is contained in the linear hull, since

$$fx \;=\; \left(\sum_{k=0}^{n} f[k]t^k\right) x \;=\; \sum_{k=0}^{n} f[k]\varphi^k(x)$$

(ii) By (i) we only have to prove $R[t]x \subseteq \mathrm{Lh}_R\{\, \varphi^k(x) \mid 0 \leq k < n \,\}$, hence consider any $gx \in R[t]x$, as f is monic we may use division with remainder to find q, $r \in R[t]$ such that $g = qf + r$ and $\deg(r) < n$ (where $r = 0$ is allowed). But as $fx = 0$ this also yields

$$gx \;=\; (qf+r)x \;=\; q(fx)+rx \;=\; rx$$

As $\deg(r) < n$ this implies that gx is contained in the linear hull of the $\varphi^k(x)$ where $0 \leq k < n$ as, analogous to the above, we may compute

$$gx \;=\; rx \;=\; \left(\sum_{k=0}^{n-1} r[k]t^k\right) x \;=\; \sum_{k=0}^{n-1} r[k]\varphi^k(x)$$

(iii) As $x \in P$ and P is φ-invariant, we have $\varphi(x) \in P$ again. By induction on $k \in \mathbb{N}$ it is clear, that $\varphi^k(x) \in P$ - for $k = 0$ we observe $\varphi^0(x) = \mathbb{1}(x) = x \in P$ by assumption. And as P is a sub-module, this implies that the linear hull of all the $\varphi^k(x)$ is contained in P. But by (i) this already is $R[t]x \subseteq P$.

In particular, if P is generated by $\{\, p_i \mid i \in I \,\}$, then we have $Rp_i \subseteq R[t]p_i \subseteq P$ and hence $P = \sum_i Rp_i \subseteq \sum_i R[t]p_i \subseteq P$ such that we have the equality of P and the sum over all $R[t]p_i$.

(iv) Choose any generating set $\{\, m_i \mid i \in I \,\}$ of M as an R-module. Then by (iii) $\{\, m_i \mid i \in I \,\}$ also is a generating set of M_φ as an $R[t]$-module. In particular we (generally) have

$$\mathrm{rank}_{R[t]}(M_\varphi) \;\leq\; \mathrm{rank}_R(M)$$

Now assume that M is finitely generated, then as we have just argued M_φ is finitely generated, as well. Then by (5.44.(iv)) there is a polynomial $f \in R[t]$ of $\deg(f) = \mathrm{rank}(M)$ such that $f(\varphi) = 0$. That is $fx = 0$ for any $x \in M$ and thereby $f \in \mathrm{ann}(M_\varphi)$. In particular $\mathrm{tor}(M_\varphi) = M_\varphi$, which means that M_φ is a torsion-module.

□

Proof of (8.39):
Fix any ordered basis of S as an R-module and let $A := [\lambda_x]$ resp. $B := [\lambda_y]$ be the basis representations

of λ_x and λ_y in this basis respectively. Then it is clear, that $\lambda_{ax}(s) = (ax)s = a(xs) = a\lambda_x(s)$ and from this we get $\lambda_{ax} = a\lambda_x$. In particular $[\lambda_{ax}] = [a\lambda_x] = a[\lambda_x]$ such that λ_{ax} has the matrix representation aA. Therefore $T_{S:R}(ax) = \mathrm{tr}(aA) = a\mathrm{tr}(A) = aT_{S:R}(x)$ and $N_{S:R}(ax) = \det(aA) = a^n\det(A) = a^n N_{S:R}(x)$, the latter as det is a multi-linear form.
In complete analogy we have $\lambda_{x+y}(s) = (x+y)s = xs + ys = \lambda_x(s) + \lambda_y(s)$ such that $\lambda_{x+y} = \lambda_x + \lambda_y$ and hence $[\lambda_{x+y}] = [\lambda_x + \lambda_y] = [\lambda_x] + [\lambda_y]$ which means, that λ_{x+y} has the matrix representation $A + B$. Therefore $T_{S:R}(x+y) = \mathrm{tr}(A+B) = \mathrm{tr}(A) + \mathrm{tr}(B) = T_{S:R}(x) + T_{S:R}(y)$. Also $\lambda_x(\lambda_y(s)) = x(ys) = (xy)s = \lambda_{xy}(s)$ such that $\lambda_x\lambda_y = \lambda_{xy}$. That is $[\lambda_{xy}] = [\lambda_x\lambda_y] = [\lambda_x][\lambda_y]$ and thereby we have found the matrix representation of λ_{xy} to be AB. Now by (4.55.(ii)) this implies

$$N_{S:R}(xy) \;=\; \det\big(\lambda_{xy}\big) \;=\; \det\big(AB\big) \;=\; \det(A)\det(B) \;=\; N_{S:R}(x)\,N_{S:R}(y)$$

By definition we have $c_x(t) = c_{\lambda_x}(t)$ and hence $c_x(\lambda_x) = 0 \in \mathrm{end}(S)$ by the Cayley-Hamilton theorem (5.44.(iii)). Yet for any $f \in R[t]$ we have $f(\lambda_x) = \lambda_{f(x)}$ and hence in particular $0 = c_x(\lambda_x) = \lambda_{c_x(x)}$ such that $c_x(x) = c_x(x)1_S = \lambda_{c_x(x)}(1_S) = 0(1_S) = 0_S$. That is $c_x(x) = 0$, as claimed. And by (5.44.(i)) we also find $T_{S:R}(x)$ and $N_{S:R}(x)$ as coefficients of $c_x(t)$, as claimed in the proposition. □

Proof of (5.42):

(i) Let $S := R[\varphi] = \mathrm{Lh}\{\,\varphi^k \mid k \in \mathbb{N}\,\} \subset \mathrm{end}(M)$ be the sub-module of $\mathrm{end}(M)$ generated by the powers of φ. Then clearly S is closed under multiplication of elements (i.e. composition of maps) and hence a ring - even a commutative ring. Let $\iota : R \hookrightarrow S$ be the canonical embedding $\iota(a) = a\mathbb{1}_M$ and $\sigma : \mathbb{N} \to S : k \mapsto \varphi^k$. Then ι is a monomorphism of rings and σ is a homomorphism of monoids. Hence by (7.14) $\sigma_\iota : f \mapsto f(\varphi)$ is a well-defined homomorphism of rings. And it is clear that $\mathrm{kn}(\sigma_\iota) = \{\,f \in R[t] \mid f(\varphi) = 0\,\} \trianglelefteq_{\mathrm{i}} R[t]$ is the null ideal of φ.

(iii) If m satisfies (a), then (1) and (2) of (b) are given already. So consider any $f \in R[t]$ such that $f \neq 0$ and $f(\varphi) = 0$. By assumption (a) we hence find some $g \in R[t]$ such that $f = gm$. In particular $g \neq 0$, as $f \neq 0$, which id $\deg(g) \geq 0$. But then $\deg(f) = \deg(gm) = \deg(g) + \deg(m)$, as R is an integral domain, and hence $\deg(f) \geq \deg(m)$.

If m satisfies (b) then (1) of (c) is given already and we need to show that m generates the null ideal of φ. As $m(\varphi) = 0$ we have $mR[t] \subseteq \{\,f \in R[t] \mid f(\varphi) = 0\,\}$. Conversely consider any $f \in R[t]$ with $f(\varphi) = 0$. As m is monic we may use division with remainder (2.67) to find some g, $r \in R[t]$ such that $f = gm + r$ and $r = 0$ or $\deg(r) < \deg(m)$. In particular

$$0 \;=\; f(\varphi) \;=\; g(\varphi)m(\varphi) + r(\varphi) \;=\; g(\varphi)\cdot 0 + r(\varphi) \;=\; r(\varphi)$$

That is $r(\varphi) = 0$ again. Suppose we had $r \neq 0$, then this would imply $\deg(m) \leq \deg(r) < \deg(m)$ by assumption (b), which is a contradiciton. Hence we have $r = 0$ and this is $f = gm \in mR[t]$.

In m satisfies (c) then (1) of (a) is given already. Also $m(\varphi) = 0$ is trivial, as $m \in mR[t] = \{\,f \in R[t] \mid f(\varphi) = 0\,\}$. So it remains to prove (3): Given $f \in R[t]$ with $f(\varphi) = 0$ we have $f \in mR[t]$ and hence $f = gm$ for some $g \in R[t]$, which already is $m \mid f$.

(ii) Suppose the null ideal $\mathfrak{z} := \{\,f \in R[t] \mid f(\varphi) = 0\,\}$ of φ is principal, that is there is some $g \in R[t]$ such that $gR[t] = \mathfrak{z}$. By the Cayley-Hamilton theorem (5.44.(iii)) we have $c_\varphi(\varphi) = 0$ and hence

$c_\varphi \in \mathfrak{z} = gR[t]$. That is there is some $f \in R[t]$ such that $c_\varphi = fg$. Yet the characteristic polynomial c_φ is monic and hence $1 = \ln(c_\varphi) = \mathrm{lc}(f) \cdot \mathrm{lc}(g)$, as R is an integral domain. That is the leading coefficient $a := \mathrm{lc}(g)$ is a unit of R and hence $m := a^{-1}g$ is a monic polynomial that generates the $\mathfrak{z}$. In particular m satisfies property (c) of (iii) and thereby $m = m_\varphi$.

(iv) Consider f, $g \in \mathfrak{v}_\varphi$, that is $0 = (fg)(\varphi) = f(\varphi)g(\varphi)$. As R is an integral domain, this means $f(\varphi) = 0$ or $g(\varphi) = 0$ such that $f \in \mathfrak{v}_\varphi$ or $g \in \mathfrak{v}_\varphi$. That makes $\mathfrak{v}_\varphi$ a prime ideal of $R[t]$. Now let m be the minimal polynomial of φ an let $m \mid fg$. By property (c) of m in (iii) this means $fg \in \mathfrak{v}_\varphi$ and as we have just seen, this implies f or $g \in \mathfrak{v}_\varphi$. By (c) again, this is nothing but $m \mid f$ or $m \mid g$, which makes m a prime element of $R[t]$.

(v) Consider any $p \in P \subseteq M$ then $m_\varphi(\varphi)(p) = 0(p) = 0$ and as this is true for any $p \in P$ we have $m_\varphi(\varphi \mid P) = 0$. By definition of a minimal polynomial of $\varphi \mid P$, this already means $m_{\varphi|P} \mid m_\varphi$.

□

Proof of (5.46):

(i) First of all $\varphi^k(x) = \lambda^k x$ is clear by induction on k: For $k = 0$ we have $\varphi^0(x) = \mathbb{1}_M(x) = x = \lambda^0 x$. Now for the induction step $\varphi^{k+1}(x) = \varphi(\varphi^k(x)) = \varphi(\lambda^k x) = \lambda^k \varphi(x) = \lambda^k \lambda x = \lambda^{k+1} x$. Using this we are able to simply compute

$$\begin{aligned} f(\varphi)(x) &= \left(\sum_{k=0}^{\infty} f[k]\varphi^k\right)(x) = \sum_{k=0}^{\infty} f[k]\big(\varphi^k(x)\big) \\ &= \sum_{k=0}^{\infty} f[k]\big(\lambda^k x\big) = \left(\sum_{k=0}^{\infty} f[k]\lambda^k\right) x = f(\lambda)\, x \end{aligned}$$

(ii) As E is a field V is free (it has a basis), according to (3.65). Also, as E is a field, the polynomial ring $E[t]$ is an Euclidean domain by (2.71.(iii)) and hence a PID, by (2.79.(iii)). Now regard

$$\mathfrak{z} := \mathrm{kn}\big(f \mapsto f(\varphi)\big) = \{\, f \in E[t] \mid f(\varphi) = 0 \,\}$$

which is an ideal in $E[t]$. By the Cayley-Hamilton theorem (5.44.(iii)) we have $c_\varphi(\varphi) = 0$, such that $\mathfrak{z} \neq 0$ is non-zero. As $E[t]$ is a PID, we can choose a generator $g \in E[t]$ of $\mathfrak{z}$. Let $a \in E$ be the leading coefficient of g, then $m := a^{-1}g \in E[t]$ is a monic generator $mF[t] = \mathfrak{z}$, too and hence we have gained the minimal polynomial $m_\varphi = m$ of φ.

(iii) *Proof without the Lemma of Gauss in case of an UFD*: Let R be an UFD and $E := \mathrm{QUOT}(R)$ be the quotient field of R. We consider $R \hookrightarrow E$ as a sub-ring of E, via $a \mapsto a/1$. Also let $c_\varphi \in R[t]$ be the characteristic polynomial of φ. By (ii) there also is a minimal polynomial $m_\varphi \in E[t]$ that is a monic generator of the ideal

$$m_\varphi E[t] = \{\, f \in E[t] \mid f(\varphi) = 0 \,\}$$

As $c_\varphi(\varphi) = 0$ by (5.44.(iii)) there is some $r_\varphi \in E[t]$ such that $c_\varphi = r_\varphi m_\varphi$. And as $c_\varphi \in R[t]$ is monic (7.29.(ix)) tells us that there are some α, $\beta \in E$ and monic polynomials $\widetilde{m}_\varphi$ and $\widetilde{r}_\varphi$ such that $m_\varphi = \alpha \widetilde{m}_\varphi$ and $r_\varphi = \beta \widetilde{m}_\varphi$ and

$$c_\varphi = \widetilde{r}_\varphi \widetilde{m}_\varphi$$

As both m_φ and $\widetilde{m}_\varphi$ are monic and $m_\varphi = \alpha\widetilde{m}_\varphi$ we find $\alpha = 1$ and hence $m_\varphi = \widetilde{m}_\varphi$. In particular $m_\varphi \in R[t]$. We will now prove that m_φ also is the minimal polynomial of φ over R: That is we consider some $f \in R[t]$, such that $f(\varphi) = 0$ and have to prove $m_\varphi \mid f$ in $R[t]$. As m_φ generates $\{ f \in E[t] \mid f(\varphi) = 0 \}$, there is some $g \in E[t]$ such that $f = g\, m_\varphi$. Yet m_φ is monic, in particular primitive. But in this situation we already get $g \in R[t]$, by (7.29.(x)) and hence $m_\varphi \mid f$ in $R[t]$.

(iii) *Proof of the general claim in case of a normal domain*: Suppose R is a normal domain and let $E := \text{QUOT}(E)$ be the quotient field of R. As before, (ii) tells us that there is a minimal polynomial m_φ of φ over E. That is m_φ is the monic generator of the ideal

$$m_\varphi E[t] \;=\; \{ f \in E[t] \mid f(\varphi) = 0 \}$$

By Cayley-Hamilton (5.44.(iii)) we also find a monic polynomial $c_\varphi \in R[t]$ such that $c_\varphi(\varphi) = 0$. In particular m_φ divides c_φ in $E[t]$. That is there is some $q \in E[t]$ such that

$$c_\varphi \;=\; q m_\varphi \;\in\; R[t]$$

As both m_φ and c_φ are monic q has to be monic, too. That is we have m_φ and $q \in E[t]$ monic polynomials, such that $qm_\varphi \in R[t]$. As R is a normal domain, this implies q, $m_\varphi \in R[t]$, according to the lemma of Gauss (8.34).

Now that we have established $m_\varphi \in R[t]$ let us check that it also is a minimal polynomial in $R[t]$. That is given any $f \in R[t]$ such that $f(\varphi) = 0$ we have to find some $g \in R[t]$ such that $f = gm_\varphi$. To do this we use division with remainder (2.67), as m_φ is monic, to write f as

$$f \;=\; g\, m_\varphi + r$$

for some g, $r \in R[t]$ with $r = 0$ or $\deg(r) < \deg(m_\varphi)$. From this we get $0 = f(\varphi) = g(\varphi)m_\varphi(\varphi) + r(\varphi) = g(\varphi) \cdot 0 + r(\varphi) = r(\varphi)$, as $m_\varphi(\varphi) = 0$. But as m_φ is the minimal polynomial in $E[t]$ this implies $m_\varphi \mid r$ in $E[t]$. That is $r = p\, m_\varphi$ for some $p \in E[t]$. Suppose we had $r \neq 0$, then $p \neq 0$ and hence $\deg(r) = \deg(p) + \deg(m_\varphi) \geq \deg(m_\varphi)$. But this contradicts $\deg(r) < \deg(m_\varphi)$, which only leaves $r = 0$. That is $f = g\, m_\varphi$ for some $g \in R[t]$, which had to be shown.

(iv) The equivalence (a) $\iff$ (d) has been proven in (5.37.(iii)). For the equivalence of (d) and (b) choose any ordered basis $\mathcal{M}$ of M and let $A := [\varphi]_{\mathcal{M}}$. Then the characteristic polynomial of φ has been defined to be the characteristic polynomial of A: $c_\varphi(t) = c_A(t) = \det(t\mathbb{1}_n - A)$. That is for any $\lambda \in R$ we have

$$c_\varphi(\lambda) \;=\; \det(\lambda\mathbb{1}_n - A)$$

Yet the determinant of $\varphi - \lambda\mathbb{1}_M$ has also been defined by choosing a basis representation and one of these is given to be $[\varphi - \lambda\mathbb{1}_M]_{\mathcal{M}} = A - \lambda\mathbb{1}_n$. Hence

$$\det(\varphi - \lambda\mathbb{1}_M) \;=\; \det(A - \lambda\mathbb{1}_n) \;=\; (-1)^n c_\varphi(\lambda)$$

and in particular, both expressions share the same roots. That is (b) is equivalent to (d), too. We now prove (c) $\implies$ (b): By the Cayley-Hamilton theorem (5.44.(iii)) we have $c_\varphi(\varphi) = 0$. By the definition of the minimal polynomial, this means $m_\varphi \mid c_\varphi$, that is $c_\varphi(t) = q(t) \cdot m_\varphi(t)$ for some

$q \in R[t]$. If now $\lambda \in R$ satisfies $m_\varphi(\lambda) = 0$, then we also get

$$c_\varphi(\lambda) \;=\; q(\lambda) \cdot m_\varphi(\lambda) \;=\; 0$$

Conversely, for (b) $\implies$ (c) we are given some $\lambda \in R$ such that $c_\varphi(\lambda) = 0$. As (b) is equivalent to (a) we can choose some $x \in M$, such that $x \neq 0$ and $\varphi(x) = \lambda x$. Then by (i) we compute

$$m_\varphi(\lambda)x \;=\; m_\varphi(\varphi)(x) \;=\; 0(x) \;=\; 0$$

where we used $m_\varphi(\varphi) = 0$, which is property (1) of the minimal polynomial. But as R is an integral domain and M is free, M also is torsion-free, due to (3.23.(ii)). Hence $m_\varphi(\lambda)x = 0$ implies $m_\varphi(\lambda) = 0$, as $x \neq 0$. And this is (c).

(v) Let $P := \mathrm{Eig}_\varphi(\lambda) \;\leq_{\mathsf{m}}\; M$, then by (5.37.(ii)) P is a φ-invariant, pure sub-module of M. As we noted there, since R is a PID, we get from (4.109.(ii)) that P is complemented, that is

$$M \;=\; P \oplus Q$$

for some sub-module $Q \;\leq_{\mathsf{m}}\; M$. Note that M is free and R is a PID, such that any sub-module $P \;\leq_{\mathsf{m}}\; M$ is free, too - according to (3.104) Likewise $Q \xrightarrow{\sim} M/P : q \mapsto q + P$ is an isomorphism and $Q \;\leq_{\mathsf{m}}\; M$ is free, such that M/P is free, too. Pick up an orered basis $\mathcal{P} = (p_1, \ldots, p_r)$ of P and an ordered basis $\mathcal{Q} = (q_1, \ldots, q_s)$ of Q. As $M = P \oplus Q$ we hence get an ordered basis $\mathcal{M} := (p_1, \ldots, p_r, q_1, \ldots, q_s)$ of M. As any $p_i \in P = \mathrm{Eig}_\varphi(\lambda)$ we have $\varphi(p_i) = \lambda p_i$ and hence the matrix representation of φ in this basis is a block-matrix of the form

$$A \;:=\; [\varphi]_{\mathcal{M}} \;=\; \begin{pmatrix} \lambda \mathbb{1}_r & B \\ 0 & D \end{pmatrix}$$

If we evaluate the characteristic polynomial of A the determinant of $t\mathbb{1}_n - A$ is the product of the determinant of $t\mathbb{1}_r - \lambda\mathbb{1}_r$ and of $t\mathbb{1}_s - D$. And thereby we find

$$(t-\lambda)^r \;=\; \det(t\mathbb{1}_r - \lambda\mathbb{1}_r) \;\mid\; \det(t\mathbb{1}_r - \lambda\mathbb{1}_r) \cdot \det(t\mathbb{1}_s - D) \;=\; \det(t\mathbb{1}_r - A) \;=\; c_A(t)$$

This means $r \leq \mathrm{AM}_\varphi(\lambda)$, the multiplicity can be even higher, as $t - \lambda$ may also divide $\det(t\mathbb{1}_s - D)$. As λ *is* an eigenvalue there is at least one eigenvector and hence $r \geq 1$. Also $r = \dim(P) = \mathrm{GM}_\varphi(\lambda)$, by construction, such that $1 \leq r = \mathrm{GM}_\varphi(\lambda) \leq \mathrm{AM}_\varphi(\lambda)$.

□

Proof of (5.57):

(i) (a) $\implies$ (b): By assumption $M_\varphi = R[t]\,x$ for any $y \in M$ there is some $g \in R[t]$ such that $y = gx$. That is

$$y \;=\; g(\varphi)(x) \;=\; \sum_{k=0}^{\infty} g[k]\varphi^k(x)$$

In particular the set $\{\, \varphi^k(x) \mid k \in \mathbb{N} \,\}$ generates M as an R-module. (b) $\implies$ (c): It suffices to show that any $\varphi^m(x)$ can be written as an R-linear combination over the set $\{\, \varphi^k(x) \mid 0 \leq k < n \,\}$. As

c_φ is monic we may use division with remainder (2.67) to find (not necessarily unique) polynomials q and $r \in R[t]$ such that $t^m = qc_\varphi + r$ and also $\deg(r) < \deg(c_\varphi) = n$. By the theorem of Cayley-Hamilton (5.44.(iii)) we have $\varphi^m = t^m(\varphi) = q(\varphi)c_\varphi(\varphi) + r(\varphi) = r(\varphi)$ and hence $\varphi^m(x) = r(\varphi)(x)$. But as $\deg(r) < n$ we see that $r(\varphi)(x)$ and hence $\varphi^m(x)$ is contained in $\mathrm{Lh}_R\{\, \varphi^k(x) \mid 0 \le k < n \,\}$. (c) $\implies$ (d): By assumption M is a free module of dimension n. As $\{\, \varphi^k(x) \mid 0 \le k < n \,\}$ also contains n elements and generates M we find that this even is a basis of M according to (3.99.(ii))

(ii) Let us denote $x_k := \varphi^{k-1}(x)$ for any $k \in 1 \ldots n$. Since $x \in M$ is a cyclic vector property (d) tells us, that $(x_1, x_2, \ldots, x_n)$ is an ordered basis of M. And we clearly have $\varphi(x_k) = \varphi(\varphi^{k-1}(x)) = \varphi^k(x) = x_{k+1}$ for any $1 \le k < n$. Also there are coefficients $a_k \in R$ where $0 \le k < n$ such that $\varphi(x_n)$ can be expressed as a linear combination

$$\varphi(x_n) \;=\; \sum_{k=1}^{n} a_k\, x_k$$

Note that $\varphi(x_n) = \varphi\varphi^{n-1}(x) = \varphi^n(x) = t^n x$ and let us define the polynomial $f \in R[t]$ of degree n by $f(t) = t^n - a_n t^{n-1} - \cdots - a_2 t - a_1$. That is f has the the coefficients $f[n] = 1$ and $f[k] = -a_{k+1}$ for $0 \le k < n$. In particular we get $fx = \varphi^n(x) - \sum_k a_k \varphi^{k-1}(x) = 0$. If now $C := \mathrm{comp}(f)$ then for $1 \le k < n$ it is clear that $Ce_k = e_{k+1}$. This matches the property $\varphi(x_k) = x_{k+1}$. We also have

$$Ce_n \;=\; \sum_{k=1}^{n}(-f[k-1])e_k \;=\; \sum_{k=1}^{n} a_k e_k$$

So $Ce_n \in R^n$ is precisely the basis representation of $\varphi(x_n)$. Altogether C is the matrix representation of φ in terms of $\mathcal{M}$.

(iii) Let us abbreviate the companion matrix of f by $C := \mathrm{comp}(f)$. In particular we have $\deg(f) = n$ as the size of C equals $\#\mathcal{M} = n$. Then by definition of the companion matrix we find

$$[\varphi(x_k)]_{\mathcal{M}} \;=\; [\varphi]_{\mathcal{M}}[x_k]_{\mathcal{M}} \;=\; Ce_k \;=\; e_{k+1} \;=\; [x_{k+1}]_{\mathcal{M}}$$

for any $1 \le k < n$. That is $\varphi(x_k) = x_{k+1}$ and by induction this yields $\varphi^k(x_1) = x_{k+1}$ for any $0 \le k < n$. For $k = n$ we compute

$$\begin{aligned}
[\varphi(x_n)]_{\mathcal{M}} \;&=\; [\varphi]_{\mathcal{M}}[x_n]_{\mathcal{M}} \;=\; Ce_n \;=\; \sum_{k=1}^{n}(-f[k-1])e_k \\
&=\; \sum_{k=0}^{n-1}(-f[k])e_{k+1} \;=\; \sum_{k=0}^{n-1}(-f[k])[\varphi^k(x_1)]_{\mathcal{M}} \\
&=\; \left[\sum_{k=0}^{n-1}(-f[k])\varphi^k(x_1)\right]_{\mathcal{M}}
\end{aligned}$$

Note that $\varphi(x_n) = \varphi(\varphi^{n-1}(x_1)) = \varphi^n(x_1)$ such that the above equation can also be written as

$$\varphi^n(x_1) \;=\; \varphi(x_n) \;=\; \sum_{k=0}^{n-1}(-f[k])\varphi^k(x_1)$$

In other words that is $fx_1 = f(\varphi)(x_1) = 0$. Also note that the x_k generate M so for any $y \in M$ there are coefficients $b_k \in R$ such that

$$y \;=\; \sum_{k=1}^{n} b_k x_k \;=\; \sum_{k=0}^{n-1} b_{k+1}\varphi^k(x_1)$$

Thus if we define $g(t) := b_1 + b_2 t + \cdots + b_n t^{n-1} \in R[t]$ then by construction we get $gx_1 = g(\varphi)(x_1) = y$. And as y was arbitrary this means that the following map is surjective

$$\varepsilon \;:\; R[t] \;\twoheadrightarrow\; M_\varphi \;:\; g \;\mapsto\; gx_1$$

But it also is $R[t]$-linear, since $\varepsilon(fg) = (fg)x_1 = f(gx_1) = f\varepsilon(g)$. As we have seen $f \in \mathrm{kn}(\varepsilon)$ since $fx_1 = 0$ such that the following map is a well defined homorphism of $R[t]$-modules

$$\bar{\varepsilon} \;:\; R[t]\Big/_{fR[t]} \;\twoheadrightarrow\; M_\varphi \;:\; g + fR[t] \;\mapsto\; gx_1$$

So it remains to prove that this map is injective. But if we let $u := t + fR[t]$ then as $\deg(f) = n$ it is clear, that $\{\, 1, u, \ldots, u^{n-1} \,\}$ generate $R[t]/fR[t]$ as an R-module. Thus any $g + fR[t]$ can be written as

$$g + fR[t] \;=\; \sum_{k=0}^{n-1} b_k u^k$$

for some $b_k \in R$. Now $\bar{\varepsilon}(u^k) = \bar{\varepsilon}(t^k + fR[t]) = t^k x_1 = \varphi^k(x_1) = x_{k+1}$. Hence $g + fR[t]$ is then mapped to

$$\bar{\varepsilon}(g + fR[t]) \;=\; \bar{\varepsilon}\left(\sum_{k=0}^{n-1} b_k u^k\right) \;=\; \sum_{k=0}^{n-1} b_k \bar{\varepsilon}(u^k) \;=\; \sum_{k=0}^{n-1} b_k x_{k+1}$$

If now $\bar{\varepsilon}(g + fR[t]) = 0$ then we can conclude $b_k = 0$ for any $0 \leq k < n$ since the x_k are a basis of M. Therefore $g + fR[t] = 0$ such that we have $\mathrm{kn}(\bar{\varepsilon}) = 0$, which is the injectivety of $\bar{\varepsilon}$.

(iv) (a) $\Longrightarrow$ (b) has been proved in (ii). (b) $\Longrightarrow$ (c) has been proved in (iii). Note that thereby the f in (c) is the same, as in (b). And for (c) $\Longrightarrow$ (a) this is easy to see: Let

$$\Phi \;:\; R[t]\Big/_{fR[t]} \;\xrightarrow{\sim}\; M_\varphi$$

be the isomorphism of $R[t]$-modules and let $x := \Phi(1 + fR[t]) \in M_\varphi$. As Φ is surjective, for any $y \in M_\varphi$ there is some $g \in R[t]$ such that $y = \Phi(g + fR[t]) = g\varphi(1 + fR[t]) = gx$. From this we see that $M_\varphi = R[t]x$ and hence $x \in M_\varphi$ is a cyclic vector.

That is we conclude (a) and hence (b) from the assumption $R[t]/fR[t] \xrightarrow{\sim} M_\varphi$. That is there is some polynomial $g \in R[t]$ such that $[\varphi] = \mathrm{comp}(g)$. But from this we can conclude $R[t]/gR[t] \xrightarrow{\sim} M_\varphi$ again. In particular $R[t]/fR[t] \cong_{\mathsf{m}} R[t]/gR[t]$ such that by (3.83.(ii)) we find $fR[t] = gR[t]$. That is $f \approx g$ and as f and g have also been assumed to be monic, we get $f = g$.

□

Proof of (5.58):

The existence of the invariant ideals has been proved in (5.32.(i)). Now for the properties of this: First of all $E[t]f_{i+1} = \mathrm{ann}(x_{i+1}) \subseteq \mathrm{ann}(x_i) = E[t]f_i$ implies $f_{i+1} \in E[t]f_i$ such that $f_i \mid f_{i+1}$ and this already

is (i). Also note that by (5.32.(i)) we also have $f_r E[t] = \mathrm{ann}(V_\varphi) = \{ f \in E[t] \mid \forall\, x \in V : fx = 0 \}$. By definition of the scalar multiplication in V_φ this is $f(\varphi)(x) = 0$ for any $x \in V$ which is equivalent to $f(\varphi)$. Altogether

$$f_r E[t] \;=\; \mathrm{ann}\big(V_\varphi\big) \;=\; \{ f \in E[t] \mid f(\varphi) = 0 \} \;=\; m_\varphi E[t]$$

That is $f_r \approx m_\varphi$ and as both f_r and m_φ are monic this implies $f_r = m_\varphi$ such that we also have established (ii). Next note, that due to $\mathrm{ann}(x_i) = f_i E[t]$ we generally have the following isomorphy of $E[t]$-modules

$$E[t] \Big/ {}_{f_i E[t]} \;\xrightarrow{\sim}\; : E[t]x_i \;:\; g + f_i E[t] \mapsto g x_i$$

as $f_i E[t] = \mathrm{ann}(x_i) = \mathrm{kn}(g \mapsto g x_i)$. As this isomorphism is E-linear, in particular, this also is an isomorphy of E-vector spaces. Therefore the dimension of $E[t]x_i$ is given to be

$$\dim_E\big(E[t]\, x_i\big) \;=\; \dim_E \Big(E[t] \Big/ {}_{f_i E[t]} \Big) \;=\; \deg(f_i) \;=\; n(i)$$

by (8.10.(i)). In the proof of (iii) and (iv) we reap the harvest of all the propositions above: By (5.56.(i)) any $E[t]x_i$ is φ-invariant. Hence the restriction $\varphi_i : E[t]x_i \to E[t]x_i$ of φ to $E[t]x_i$ is well-defined. Hereby x_i is a cyclic vector of $E[t]x_i$ by (5.57.(i)) and hence we have $[\varphi_i]_{\mathcal{M}_i} = \mathrm{comp}(f)$ for some monic polynomial f by (5.57.(iv)). Thereby $f = f_i$, as $E[t]/f_i E[t] \xrightarrow{\sim} E[t]x_i$ are isomorphic, as $E[t]$-modules and these polynomials are the same. Now we use (5.48.(iii)) to find statement (iii)

$$c_\varphi \;=\; \prod_{i=1}^{r} c_{\varphi_i}$$

As x_i is a cyclic vector for $E[t]x_i$ and this subspace has dimension $n(i)$ over E, we find that $\mathcal{V}_i$ truly is an ordered basis. By (5.57.(ii)) we then find $[\varphi_i]_{\mathcal{V}_i} = \mathrm{comp}(g_i)$ for some monic polynomial g_i of degree $n(i)$ with $g_i x_i = 0$ again. That is $g_i \in \mathrm{ann}(x_i) = f_i E[t]$, and as $\deg(f_i) = n_i$ this implies $f_i \approx g_i$ and as both are monic $g_i = f_i$ again. That is $[\varphi_i]_{\mathcal{V}_i} = \mathrm{comp}(f_i)$ and hence we find (iv)

$$[\varphi]_{\mathcal{V}} \;:\; \bigoplus_{i=1}^{r} [\varphi_i]_{\mathcal{V}_i} \;=\; \bigoplus_{i=1}^{r} \mathrm{comp}(f_i)$$

□

Proof of (5.60):
Statement (i) is just (3.146.(v)) and statement is just (3.160.(i)). Δ_φ is a well-defined homomorphism of R-modules, as it is $\Delta_\varphi = \lambda_t \otimes M + R[t] \otimes \varphi$. And π_φ comes from the R-bilinear map $(f, x) \mapsto fx$ by the universal property of the tensor product. Let us also verify the $R[t]$-linearity of these maps:

$$\begin{aligned}
\Delta_\varphi\big(g(f \otimes x)\big) \;&=\; \Delta_\varphi\big((gf) \otimes x\big) \;=\; (tgf) \otimes x + (gf) \otimes \varphi(x) \\
&=\; g\big((tf) \otimes x + f \otimes \varphi(x)\big) \;=\; g\, \Delta_\varphi\big(f \otimes x\big) \\
\pi_\varphi\big(g(f \otimes x)\big) \;&=\; \pi_\varphi\big((gf) \otimes x\big) \;=\; (gf)x \;=\; g(fx) \;=\; g\, \pi_\varphi\big(f \otimes x\big)
\end{aligned}$$

(iii) The surjectivity of π_φ is clear: Given any $x \in M$ this is contained in the image, as $\pi_\varphi(\mathbf{1} \otimes x) = \mathbf{1}x = \mathbb{1}(x) = x$. Next we prove the injectivity of Δ_φ: By (i) any element of $M_{R[t]}$ can be written as

a finite sum of $t^k \otimes x_k$ uniquely. Now suppose

$$\begin{aligned} 0 &= \Delta_\varphi\left(\sum_{k=0}^{d} t^k \otimes x_k\right) = \sum_{k=0}^{d} \left(t^{k+1} \otimes x_k - t^k \otimes \varphi(x_k)\right) \\ &= \sum_{k=1}^{d+1} t^k \otimes x_{k-1} - \sum_{k=0}^{d} t^k \otimes \varphi(x_k) = t^{d+1} \otimes x_d + \sum_{k=1}^{d} t^k \otimes \left(x_{k-1} - \varphi(x_k)\right) - \mathbf{1} \otimes \varphi(x_0) \end{aligned}$$

As $0 = \sum_k t^k \otimes 0$ as well and the x_k are uniquely determined we find $x_d = 0$ by comparing the tensor-companion of t^{d+1} and for any $k \in 1 \dots n$ also $x_{k-1} = \varphi(x_k)$ by comparing the tensor-companions of t^k. That is $x_{d-1} = \varphi(x_d) = \varphi(0) = 0$ and so on, such that we get $x_k = 0$ for any $k \in 0 \dots d$. That is $\mathsf{kn}(\Delta_\varphi) = 0$ and hence Δ_φ is injective.

(iii) Let us check $\mathsf{im}(\Delta_\varphi) \subseteq \mathsf{kn}(\pi_\varphi)$ next: That is we have to verify $\pi_\varphi \Delta_\varphi = 0$ and for this it suffices to regard elements of the form $t^k \otimes x$, as these generate $M_{R[t]}$. So let us compute

$$\begin{aligned} \pi_\varphi \Delta_\varphi\left(t^k \otimes x\right) &= \pi_\varphi\left(t^{k+1} \otimes x - t^k \otimes \varphi(x)\right) \\ &= t^{k+1}x - t^k\varphi(x) = \varphi^{k+1}(x) - \varphi^k\left(\varphi(x)\right) = 0 \end{aligned}$$

(iii) The exactness of the chain is established, once we prove $\mathsf{kn}(\pi_\varphi) \subseteq \mathsf{im}(\Delta_\varphi)$: To do this let us first prove that for any $k \geq 1$ and any $x \in M$ we have $t^k \otimes x - \mathbf{1} \otimes \varphi^k(x) \in \mathsf{im}(\Delta_\varphi)$. This can be done by a simple telescope sum

$$\begin{aligned} \Delta_\varphi\left(\sum_{r=0}^{k-1} t^{k-1-r} \otimes \varphi^r(x)\right) &= \sum_{r=0}^{k-1} \Delta_\varphi\left(t^{k-1-r} \otimes \varphi^r(x)\right) \\ &= \sum_{r=0}^{k-1} \left(t^{k-r} \otimes \varphi^r(x) - t^{k-1-r} \otimes \varphi^{r+1}(x)\right) \\ &= \sum_{r=0}^{k-1} \left(t^{k-r} \otimes \varphi^r(x)\right) - \sum_{r=1}^{k} \left(t^{k-r} \otimes \varphi^r(x)\right) \\ &= t^k \otimes x - \mathbf{1} \otimes \varphi^k(x) \end{aligned}$$

We use this to prove $x \in \mathsf{im}(\Delta_\varphi)$ for any $x \in \mathsf{kn}(\pi_\varphi)$: If $x = \sum_k t^k \otimes x_k$ then $\pi_\varphi(x) = 0$ means

$$0 = \sum_{k=0}^{d} t^k x_k = \sum_{k=0}^{d} \varphi^k(x_k)$$

But this property enables us to append x to $x + 0$ is such a way that it becomes apparent, that x is contained in the image of Δ_φ using the telescope elements above

$$\begin{aligned} x &= \sum_{k=0}^{d} t^k \otimes x_k = \sum_{k=0}^{d} t^k \otimes x_k - \mathbf{1} \otimes 0 \\ &= \sum_{k=0}^{d} t^k \otimes x_k - \mathbf{1} \otimes \left(\sum_{k=0}^{d} \varphi^k(x_k)\right) \\ &= \sum_{k=0}^{d} \left(t^k \otimes x_k - \mathbf{1} \otimes \varphi^k(x_k)\right) \in \mathsf{im}(\Delta_\varphi) \end{aligned}$$

(iv) If M is generated by $\{ m_i \mid i \in I \}$ as an R-module, then $M_{R[t]}$ is generated by $\{ \mathbf{1} \otimes m_i \mid i \in I \}$ as an $R[t]$-module. As Δ_φ is injective, it becomes an isomorphism, when restricted to its image

$$\Delta_\varphi \;:\; M_{R[t]} \;\xrightarrow{\sim}\; \mathrm{im}(\Delta_\varphi) \;=\; \mathrm{kn}(\pi_\varphi)$$

In particular the generating set $\{ \mathbf{1} \otimes m_i \mid i \in I \}$ of $M_{R[t]}$ is transferred into $\mathrm{kn}(\pi_\varphi)$ under Δ_φ. And as $\Delta_\varphi(\mathbf{1} \otimes m_i) = t \otimes m_i - \mathbf{1} \otimes \varphi(m_i)$ by definition of Δ_φ we find, that the set given in the claim of (iv) truly generates $\mathrm{kn}(\pi_\varphi)$ as an $R[t]$-module.

(v) Let $\mathcal{M} = (m_1, \ldots, m_n)$ be an ordered R-basis of M, then by (ii) $\mathbf{1} \otimes \mathcal{M} := (\mathbf{1} \otimes m_1, \ldots, \mathbf{1} \otimes m_n)$ is an ordered $R[t]$-basis of $M_{R[t]}$. Let $A := [\varphi] \in \mathrm{mat}_n(R)$ be the representation of φ with respect to $\mathcal{M}$, that is for any $j \in 1 \ldots n$ we have

$$\varphi(m_j) \;=\; \sum_{i=1}^{n} a_{i,j} m_i$$

From this we will deduce that the matrix representation of Δ_φ with respect to $\mathbf{1} \otimes \mathcal{M}$ is given by $(t\mathbb{1}_n - A) \in \mathrm{mat}_n(R[t])$ (see below). And from this we immediately get the identity of the determinant: $\det(\Delta_\varphi) = \det(t\mathbb{1}_n - A) = c_\varphi(t)$. So let us verify $[\Delta_\varphi] = (t\mathbb{1}_n - A)$:

$$\begin{aligned}
\Delta_\varphi(\mathbf{1} \otimes m_j) &= t \otimes m_j - \mathbf{1} \otimes \varphi(m_j) \\
&= t \otimes m_j - \mathbf{1} \left(\sum_{i=1}^{n} a_{i,j} m_i \right) \\
&= t\,\mathbf{1} \otimes m_j - \sum_{i=1}^{n} a_{i,j}\,\mathbf{1} \otimes m_i \\
&= \sum_{i=1}^{n} \left(t\delta_{i,j} - a_{i,j} \right) \mathbf{1} \otimes m_i \\
&= \sum_{i=1}^{n} \left[t\mathbb{1}_n - A \right]_{i,j} \mathbf{1} \otimes m_i
\end{aligned}$$

□

Proof of (5.48):

(i) Pick up an ordered basis $\mathcal{M} = (m_1, \ldots, m_r)$ of M and let $\mathcal{N} := (n_1, \ldots, n_r)$ where $n_i := \Phi(m_i)$. As Φ is an isomorphism it is clear that $\mathcal{N}$ is an ordered basis of N. And by construction $\Phi(m_i) = n_i$ we have $[\Phi]^{\mathcal{N}}_{\mathcal{M}} = \mathbb{1}_r$. Thus

$$[\psi]_{\mathcal{N}} \;=\; [\Phi\psi\Phi^{-1}]_{\mathcal{N}} \;=\; [\Phi]^{\mathcal{N}}_{\mathcal{M}}\, [\varphi]_{\mathcal{M}}\, [\Phi^{-1}]^{\mathcal{M}}_{\mathcal{N}} \;=\; \mathbb{1}_r\, [\varphi]_{\mathcal{M}}\, \mathbb{1}_r \;=\; [\varphi]_{\mathcal{M}}$$

That is ψ and φ share the same matrix representation $A := [\varphi]_{\mathcal{M}} = [\psi]_{\mathcal{N}}$ and in particular the same characteristic polynomial $c_\varphi(t) = c_A(t) = c_\psi(t)$.

(i) Let us first prove that $\psi^k = \Phi\varphi^k\Phi^{-1}$ by induction on k: The case $k = 0$ is easy, as $\psi^0 = \mathbb{1}_N$ and $\Phi\varphi^0\Phi^{-1} = \Phi\mathbb{1}_M\Phi^{-1} = \mathbb{1}_N$ in this case. And for the induction step we simply compute

$$\psi^{k+1} \;=\; \psi^k\psi \;=\; \Phi\varphi^k\Phi^{-1}\,\Phi\varphi\Phi^{-1} \;=\; \Phi\varphi^k\varphi\Phi^{-1} \;=\; \Phi\varphi^{k+1}\Phi^{-1}$$

As Φ is R-linear and as the addition and scalar multiplication in $\mathrm{end}(M)$ are point-wise, we find $f(\psi) = f(\Phi\varphi\Phi^{-1}) = \Phi f(\varphi)\Phi^{-1}$ for any polynomial $f \in R[t]$, as for any $y \in N$ we compute

$$\begin{aligned} f(\psi)(y) &= \sum_{k=0}^{\infty} f[k]\psi^k = \sum_{k=0}^{\infty} f[k]\Phi\varphi^k\Phi^{-1}(y) = \left(\sum_{k=0}^{\infty} f[k]\Phi\varphi^k\right)\left(\Phi^{-1}(y)\right) \\ &= \Phi\left(\sum_{k=0}^{\infty} f[k]\varphi^k\right)\left(\Phi^{-1}(y)\right) = \Phi f(\varphi)\left(\Phi^{-1}(y)\right) = \Phi f(\varphi)\Phi^{-1}(y) \end{aligned}$$

In particular we find the equivalence of $f(\psi) = 0 \in \mathrm{end}(N)$ and $f(\varphi) = 0 \in \mathrm{end}(M)$, as for any $y = \Phi(x) \in N$ we have the following equivalence

$$\begin{aligned} f(\sigma)(y) = 0_N &\iff \Phi f(\varphi)\Phi^{-1}(y) = 0_N \\ &\iff f(\varphi)\Phi^{-1}(y) = 0_M \\ &\iff f(\varphi)(x) = 0_M \end{aligned}$$

as Φ is assumed to be bijective. That is the ideals $\mathrm{kn}(f \mapsto f(\psi)) = \{ f \in R[t] \mid f(\psi) = 0_N \}$ and $\mathrm{kn}(f \mapsto f(\varphi)) = \{ f \in R[t] \mid f(\varphi) = 0_M \}$ are identical subsets of $R[t]$. However m_ψ and m_φ are the monic generators of the respective ideal(s) and hence they have to be identical, too.

(ii) First of all $\varphi \mid P$ i well-defined, as $\varphi(P) \subseteq P$ by assumption. Also $\overline{\varphi}$ is well-defined: If $x + P = y + P$ then $y - x \in P$ such that $\varphi(y) - \varphi(x) = \varphi(y - x) \in \varphi(P) \subseteq P$ and therefore $\varphi(y) + P = \varphi(x) + P$.

By assumption P is free, so there is a basis $\{ p_i \mid i \in I \}$ of P. According to (3.99.(iv)) $|I| = \dim(P) \leq \mathrm{rank}(M) < \infty$ as M was assumed to be finitely generated. Thus we may take $I = 1 \ldots r$. By assumption also M/P is free as well, so there is a basis $\{ q_j + P \mid j \in J \}$ of M/P. Thereby $\{ q_j \mid j \in J \}$ is linearly independent, as $\sum_j b_j q_j = 0$ would imply $\sum_j b_j(q_j + P) = 0 + P$ and hence $b_j = 0$ for any $j \in J$. Thus (3.99.(iv)) also implies $|J| < \infty$ and we may take $J = 1 \ldots s$. Then we find, that $\{ p_1, \ldots, p_r \} \cup \{ q_1, \ldots, q_s \}$ is a basis of M, as any $x \in M$ can be uniquely written, as

$$x = \sum_{i=1}^{r} a_i p_i + \sum_{j=1}^{s} b_j q_j$$

where $x + P = \sum_j b_j(q_j + P)$ and $x - \sum_j b_j q_j = \sum_i a_i p_i \in P$. Let us denote $\mathcal{M} := (p_1, \ldots, p_r, q_1, \ldots, q_s)$ and likewise $\mathcal{P} := (p_1, \ldots, p_r)$ and $\mathcal{Q} := (q_1 + P, \ldots, q_s + P)$. Then $\mathcal{M}$ is an ordered basis of M, $\mathcal{P}$ is an ordered basis of P and $\mathcal{Q}$ is an ordered basis of M/P. Since P is invariant under φ we have $\varphi(p_i) \in P = \mathrm{Lh}\{ p_1, \ldots, p_r \}$. Therefore the matrix representation of φ in this basis is of the following form:

$$D := [\varphi]_{\mathcal{M}} = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} \in \mathrm{mat}_{r+s}(R)$$

For some matrices $A \in \mathrm{mat}_r(R)$, $B \in \mathrm{mat}_{r,s}(R)$ and $C \in \mathrm{mat}_s(R)$. By construction it is clear, that $A = [\varphi \mid P]_{\mathcal{P}}$. But also $[\overline{\varphi}]_{\mathcal{Q}} = C$, as $\overline{\varphi}(q_j + P) = \varphi(q_j) + P$. Thus we may compute the characteristic polynomial of φ by evaluating the characteristic polynomial of D. For the determinant

of the block matrix $t\mathbb{1}_{r+s} - D$ we thereby use (4.58.(i))

$$\begin{aligned} c_D(t) &= \det\big(t\mathbb{1}_{r+s} - D\big) = \det\begin{pmatrix} t\mathbb{1}_r - A & -B \\ 0 & t\mathbb{1}_s - C \end{pmatrix} \\ &= \det(t\mathbb{1}_r - A)\cdot\det(t\mathbb{1}_s - C) = c_A(t)\cdot c_C(t) \end{aligned}$$

As the characteristic polynomials can be computed for *any* basis representation we have $c_\varphi(t) = c_D(t) = c_A(t)\cdot c_C(t) = c_{\varphi|P}(t)\cdot c_{\overline{\varphi}}(t)$.

(iii) For the proof of this statement we use induction on r, the case $r = 1$ being trivial. For $r+1$ let us denote $P := P_{r+1}$ and $Q := P_1 + \cdots + P_r$. Then $M = P \oplus Q$ and in particular we have the isomorphism

$$\Phi : Q \xrightarrow{\sim} M\Big/_P : q \mapsto q + P$$

In particular M/P is free again, as all the P_i admit a basis. Hence the requirements of (ii) are satisfied and we pick up $\overline{\varphi} \in \mathrm{end}(M/P)$. Then for any $q \in Q$ we have $\Phi(\varphi \mid Q)(q) = \varphi(q) + P$ and $\overline{\varphi}\Phi(q) = \overline{\varphi}(q+P) = \varphi(q) + P$ such that $\Phi(\varphi \mid Q) = \overline{\varphi}\Phi$. From this we get $\overline{\varphi} = \Phi(\varphi \mid Q)\Phi^{-1}$ such that (i) implies $c_{\overline{\varphi}}(t) = c_{\varphi|Q}$. By the induction hypothesis for $\varphi \mid Q$ we then get

$$c_\varphi(t) = c_{\varphi|P}(t)\cdot c_{\overline{\varphi}}(t) = c_{\varphi|P}(t)\cdot c_{\varphi|Q}(t) = c_{\varphi|P_{r+1}}(t)\cdot\prod_{i=1}^{r} c_{\varphi_i}(t)$$

(iv) ($\diamondsuit$) This proof is computational, yet a little advanced. It is based on the machinery provided in proposition (5.60), so the reader should familiarize himself with the notation used there.

Now pick up an ordered basis $\mathcal{M} := (m_1, \ldots, m_n)$ of the R-module M. Then by (5.60.(ii)) we also obtain an ordered $R[t]$-basis of $M_{R[t]}$ by $\mathbf{1}\otimes\mathcal{M} := (\mathbf{1}\otimes m_1, \ldots, \mathbf{1}\otimes m_n)$. By assumption, for any $k \in 1\ldots n$, we have $f_k\,\mathbf{1}\otimes m_k = f_k \otimes m_k \in \mathrm{kn}(\pi_\varphi)$, since

$$\pi_\varphi\big(f_k\otimes m_k\big) = f_k m_k = f_k(\varphi)(m_k) = 0(m_k) = 0$$

But by (5.60.(iii)) we have $\mathrm{kn}(\pi_\varphi) = \mathrm{im}(\Delta_\varphi)$ and by (5.60.(iv)) the image of Δ_φ is generated (as an $R[t]$-module) by elements of the form $t\otimes m_j - \mathbf{1}\otimes\varphi(m_j)$. That is there are polynomials $g_{j,k} \in R[t]$ such that

$$f_k\,\mathbf{1}\otimes m_k = \sum_{j=1}^{n} g_{j,k}\left(t\otimes m_j - \mathbf{1}\otimes\varphi(m_j)\right)$$

Let $A = [\varphi]$ be the representation of φ with respect to the basis $\mathcal{M}$. That is $\varphi(m_j) = \sum_i a_{i,j}m_i$ for any $j \in 1\ldots n$. Then we can insert $\varphi(m_j)$ into the equation above

$$\begin{aligned} f_k\,\mathbf{1}\otimes m_k &= \sum_{j=1}^{n} g_{j,k}\left(t\otimes m_j - \mathbf{1}\otimes\left(\sum_{i=1}^{n} a_{i,j}m_i\right)\right) \\ &= \sum_{j=1}^{n} g_{j,k}\left(t\,\mathbf{1}\otimes m_j - \sum_{i=1}^{n} a_{i,j}\,\mathbf{1}\otimes m_i\right) \\ &= \sum_{j=1}^{n} g_{j,k}\sum_{i=1}^{n}\left(\delta_{i,j}t\,\mathbf{1}\otimes m_i - a_{i,j}\,\mathbf{1}\otimes m_i\right) \end{aligned}$$

$$
\begin{aligned}
&= \sum_{j=1}^{n} g_{j,k} \sum_{i=1}^{n} \left(\delta_{i,j} t - a_{i,j}\right) \mathbf{1} \otimes m_i \\
&= \sum_{i=1}^{n} \left(\sum_{j=1}^{n} \left(\delta_{i,j} t - a_{i,j}\right) g_{j,k} \right) \mathbf{1} \otimes m_i
\end{aligned}
$$

Let $G := (g_{j,k}) \in \mathrm{mat}_n(R[t])$ be the matrix composed of the coefficient polynomials $g_{j,k}$ then the equation above tells us that the coefficients of the basis representation of $f_k \mathbf{1} \otimes m_k$ in $\mathbf{1} \otimes \mathcal{M}$ are precisely the coefficients of the matrix multiplication $(t\mathbb{1}_n - A)G$

$$
f_k \mathbf{1} \otimes m_k \;=\; \sum_{i=1}^{n} \left(\sum_{j=1}^{n} [t\mathbb{1}_n - A]_{i,j} [G]_{j,k} \right) \mathbf{1} \otimes m_i \;=\; \sum_{i=1}^{n} \left[\left(t\mathbb{1}_n - A\right) G \right]_{i,k} \mathbf{1} \otimes m_i
$$

Let $F := \mathrm{dia}(f_1, \ldots, f_n)$ be the diagonal matrix of the polynomials f_k, then the left hand side is the basis representation of the k-th row of F. The right hand side is the k-th row of the basis representation of $(t\mathbb{1}_n - A)G$. That is we have found the following identity of matrices

$$
F \;=\; \left(t\mathbb{1}_n - A\right) G
$$

And from this identity, as the determinant is multiplicative, we find that the characteristic polynomial of φ is a factor of the product $f_1 \ldots f_n$, the other being the determinant of G

$$
f_1 \cdot \ldots \cdot f_n \;=\; \det\left(F\right) \;=\; \det\Big(\left(t\mathbb{1}_n - A\right) G\Big) \;=\; \det\left(t\mathbb{1}_n - A\right)\det\left(G\right) \;=\; c_\varphi \det\left(G\right)
$$

(v) Since the row in the diagram is exact φ injective and hence we have an isomorphism $\Phi : L \xrightarrow{\sim} P := \mathrm{im}(\varphi) : x \mapsto \varphi(x)$. And as the diagram commutes we have $\mu\varphi = \varphi\lambda$. Thus if $y = \varphi(x) \in P$ then $\mu(y) = \mu\varphi(x) = \varphi\lambda(x) \in \mathrm{im}(\varphi) = P$. That is $\mu(P) \subseteq P$ and thereby we may regard the map $\mu \mid P$. For this we also get $(\mu \mid P)\Phi = \Phi\lambda$ such that $\mu \mid P = \Phi\lambda\Phi^{-1}$. In particular (i) implies

$$
c_{\mu|P}(t) \;=\; c_\lambda(t)
$$

The exactness of the rows also means $P = \mathrm{im}(\varphi) = \mathrm{kn}(\psi)$ and therefore we obtain another isomorphism

$$
\Psi \;:\; M \Big/ P \;\xrightarrow{\sim}\; N \;:\; y + P \;\mapsto\; \psi(y)
$$

As N is free, so is M/P. That is all the requirements of (ii) for μ with P are satisfied. Therefore we find the split

$$
c_\mu(t) \;=\; c_{\mu|P}(t) \cdot c_{\overline{\mu}}(t)
$$

The commutativity of the right side of the diagram is $\nu\psi = \psi\mu$. Thus $\Psi\overline{\mu}(y + P) = \Psi(\mu(y) + P) = \psi\mu(y)$ and $\nu\Psi(y + P) = \nu\psi(y)$ such that $\Psi\overline{\mu} = \nu\Psi$ as well. Therefore we also found $\nu = \Psi\overline{\mu}\Psi^{-1}$ and by (i)

$$
c_{\overline{\mu}}(t) \;=\; c_\nu(t)
$$

Altogether we have found three equalities of characteristic polynomials that finally yield the desired result: $c_\mu(t) = c_{\mu|P}(t) \cdot c_{\overline{\mu}}(t) = c_\lambda(t) \cdot c_\nu(t)$.

(vi) If $\mathcal{M} = (m_1, \ldots, m_n)$ is an ordered R-basis of M, then according to (3.160.(i)) $\mathcal{M}_S := (1 \otimes m_1, \ldots, 1 \otimes m_n)$ is an ordered S basis of M_S. And if $A = (a_{i,j}) = [\varphi]_{\mathcal{M}}$ is the representation of φ in this basis, then φ_S has the representation $[\varphi_S]_{\mathcal{M}_S} = \alpha(A) := (\alpha(a_{i,j}))$ as we have seen in (3.160.(ii)). In particular

$$c_{\varphi_S}(t) \;=\; \det\big(t\mathbb{1}_n - \alpha(A)\big) \;=\; \det\big(\widetilde{\alpha}(t\mathbb{1}_n - A)\big)$$

Now $\widetilde{\alpha}$ is a homomorphism of rings, since α was assumed to be such. And as the determinant can be computed explicitly by a combination of sums and products, we can pull $\widetilde{\alpha}$ out of the determinant (this is (4.55).(vi)). Doing this we arrive at

$$c_{\varphi_S}(t) \;=\; \det\big(\widetilde{\alpha}(t\mathbb{1}_n - A)\big) \;=\; \widetilde{\alpha}\big(\det(t\mathbb{1}_n - A)\big) \;=\; \widetilde{\alpha}\big(c_\varphi(t)\big)$$

□

Proof of (5.52):

- Let us first prove the equivalences of (a), (b) and (c) in case of a general commutative ring R: Starting with (a) there is a basis $\{ m_1, \ldots, m_n \}$ such that $\varphi(m_i) = \lambda_i m_i$. We order this basis arbitrarily, say $\mathcal{M} := (m_1, \ldots, m_n)$. Then $\varphi(m_i) = \lambda_i m_i$ tells us that $[\varphi(m_i)]_{\mathcal{M}} = \lambda_i e_i$. That means $[\varphi]_{\mathcal{M}} = \mathrm{dia}(\lambda_1, \ldots, \lambda_n)$ is a diagonal matrix, such that we have arrived at (b). Now consider any (other) ordered basis $\mathcal{M}'$ of M. We want to prove that $[\varphi]_{\mathcal{M}'}$ is diagonizable and start with a diagonal matrix $D = [\varphi]_{\mathcal{M}}$. By change of base (4.42.(v)) we let $T := [\mathbb{1}_M]^{\mathcal{M}'}_{\mathcal{M}}$ and hence find

$$[\varphi]_{\mathcal{M}'} \;=\; T\,D\,T^{-1} \;\approx\; D$$

That is we have arrived at (c): $[\varphi]_{\mathcal{M}'}$ is diagonizable. Now we need to return to (a). That is we have $A = [\varphi]_{\mathcal{M}'} = TDT^{-1}$ for some diagonal matrix $D = \mathrm{dia}(\lambda_1, \ldots, \lambda_n)$ and need to find a basis $\{ m_1, \ldots, m_n \}$ of M such that $\varphi(m_i) = \lambda_i m_i$. Let $\mathcal{M}' = (m'_1, \ldots, m'_n)$ and $A = (a_{i,j})$, likewise $T = (t_{i,j})$ and for any $j \in 1 \ldots n$ define

$$m_j \;:=\; \sum_{i=1} t_{i,j}\, m'_i$$

As T is invertible (4.42.(iii)) tells us that $\mathcal{M} := (m_1, \ldots, m_n)$ truly is an ordered basis of M and that $T = [\mathbb{1}_M]^{\mathcal{M}'}_{\mathcal{M}}$ and $T^{-1} = [\mathbb{1}_M]^{\mathcal{M}}_{\mathcal{M}'}$ are the matrices of base change. Thus we have

$$[\varphi(m_j)]_{\mathcal{M}} \;=\; [\varphi]_{\mathcal{M}}[m_j]_{\mathcal{M}} \;=\; [\mathbb{1}_M]^{\mathcal{M}}_{\mathcal{M}'}\,[\varphi]_{\mathcal{M}'}\,[\mathbb{1}_M]^{\mathcal{M}'}_{\mathcal{M}}[m_j]_{\mathcal{M}} \;=\; T^{-1}\,A\,T\,e_j \;=\; De_j \;=\; \lambda_j e_j$$

Returning from the basis representation of $\mathcal{M}$ (using $R^n \xrightarrow{\sim} M : a \mapsto a_1 m_1 + \ldots a_n m_n$ the inverse isomorphism) we see $\varphi(m_j) = \lambda_j m_j$ which is (a). In the end we have come full circle.

- Let us now assume, that R is an integral domain, then we will prove (a) $\Longrightarrow$ (e), (e) $\Longrightarrow$ (d) is trivial and we will return by proving (d) $\Longrightarrow$ (e) and (e) $\Longrightarrow$ (c). As (a) and (c) are equivalent, this suffices. The easy part is from (a) to (e):

 If $\{ m_1, \ldots, m_n \}$ is a basis of M such that $\varphi(m_j) = a_j m_j$ we have already seen in example (5.36)

that for any $\lambda \in R$ the eigenspace of φ to λ is given to be

$$\mathrm{Eig}_\varphi(\lambda) \;=\; \mathrm{Lh}\{\, m_j \mid j \in 1 \ldots n,\, a_j = \lambda \,\}$$

Let us denote the distinct elements of the a_j by λ_i again, that is $\{\, a_1, \ldots, a_n \,\} = \{\, \lambda_1, \ldots, \lambda_r \,\}$. Then it is clear that we get a partition of $\{\, m_1, \ldots, m_n \,\} = \mathcal{M}_1 \cup \cdots \cup \mathcal{M}_r$ by taking

$$\mathcal{M}_i \;:=\; \left\{\, m_j \mid j \in 1 \ldots n,\, a_j = \lambda_i \,\right\}$$

and as the $\mathcal{M}_i$ are linearly independent and generate $\mathrm{Eig}_\varphi(\lambda_i)$ they even are a basis of the respective $\mathrm{Eig}_\varphi(\lambda_i)$. In particular any $\mathrm{Eig}_\varphi(\lambda_i)$ is a free sub-module and we have decomposed into an inner direct sum

$$M \;=\; \bigoplus_{i=1}^{r} \mathrm{Eig}_\varphi(\lambda_i)$$

This is (e) and in particular M is the sum of the eigenspaces, which is (d). Just to be sure: Any $x \in M$ can be expressed (in a unique way), as a sum of the form

$$x \;=\; \sum_{j=1}^{n} x_j m_j \;=\; \sum_{i=1}^{r} \sum_{m_j \in \mathcal{M}_i} x_j m_j$$

We now want to prove (e) from (d), that is we have to prove that the sum is direct, automatically, as we deal with eigenspaces. For ease of notation consider some

$$x_1 \;\in\; \mathrm{Eig}_\varphi(\lambda_1) \cap \sum_{i=2} \mathrm{Eig}_\varphi(\lambda_i)$$

That is there are some $x_i \in \mathrm{Eig}_\varphi(\lambda_i)$ (for $i \in 2 \ldots r$) such that $x_1 = x_2 + \cdots + x_r$. If we had $x_1 \neq 0$ then there would have to be one or more $x_i \neq 0$ for $i \in 2 \ldots r$. Yet $1 \neq 0 \in R$ and by (5.37.(iv)) non-zero x_i would be linearly independent. Thus we find $x_1 = 0$ and hence conclude (e) again.

It remains to prove (c) from (e): As the eigenspaces $M_i := \mathrm{Eig}_\varphi(\lambda_i)$ are free by assumption (e) we can choose bases $\mathcal{M}_i = \left\{\, m_{i,j} \mid j \in 1 \ldots s(i) \,\right\}$ for M_i each. This enables us to decompose M further, into the inner direct sum

$$M \;=\; \bigoplus_{i=1}^{r} M_i \;=\; \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{s(i)} R m_{i,j}$$

As $m_{i,j} \in M_i$ we get $\varphi(m_{i,j}) = \lambda_i m_{i,j} \in R m_{i,j}$ which means that all the $R m_{i,j}$ are invariant under φ. And of course $R m_{i,j}$ is free, as $\left\{\, m_{i,j} \,\right\}$ is its basis. In particular we find that $\mathcal{M} := \left\{\, m_{i,j} \mid i \in 1 \ldots r,\, j \in 1 \ldots s(i) \,\right\}$ is a basis of M and hence $s(1) + \cdots + s(r) = n$. Let $A := [\varphi]_{\mathcal{M}}$ be the representation of φ with respect to this basis. By (4.46.(iii)) we find that

$$A \;\approx\; D \;:=\; A_1 \oplus \cdots \oplus A_n$$

where any A_j is a matrix of size 1. Clearly D is a diagonal matrix, by construction and hence A is similar to a diagonal matrix. If now $\mathcal{M}'$ is any other ordered basis of M, then by (4.42.(v)) $[\varphi]_{\mathcal{M}'}$

is similar to $A = [\varphi]_{\mathcal{M}}$, as well. Hence $[\varphi]_{\mathcal{M}'}$ is diagonizable, as $\approx$ is a transitive relation:

$$[\varphi]_{\mathcal{M}'} \approx [\varphi]_{\mathcal{M}} \text{ and } [\varphi]_{\mathcal{M}} \approx D \implies [\varphi]_{\mathcal{M}'} \approx D$$

- Let us assume R is a field, that we have to prove that (f) and (g) imply (a). In this item we start with (g) $\implies$ (a), that is we assume that the minimal polynomial m_φ splits into *distinct* factors

$$m_\varphi(t) = (t-\lambda_1)(t-\lambda_2)\dots(t-\lambda_r)$$

We will prove, that (a) under this assumption, by induction on the dimension $n := \dim(M)$ of M as an R-vector-space. For $n = 1$ any endomorphism satisfies (a), as $\varphi(a) = \lambda a$ for $\lambda = \varphi(1)$. So let us assume $n > 1$ and proceed by defining

$$L_1 := \operatorname{im}(\varphi - \lambda_1 \mathbb{1})$$

If $L_1 = 0$ then $\varphi = \lambda_1 \mathbb{1}$ and hence we are done already. Thus we are only concerned with $L_1 \neq 0$. First of all, by the dimension formula (3.68.(iii)) we have

$$\dim(L_1) = \dim(V) - \dim\big(\ker(\varphi - \lambda_1\mathbb{1})\big) = n - \mathrm{GM}_\varphi(\lambda_1) < 1$$

Also L_1 is φ-invariant: Consider any $y := \varphi(x) - \lambda_1 x \in L_1$ then $\varphi(y) = \varphi(\varphi - \lambda_1\mathbb{1})(x) = (\varphi - \lambda_1\mathbb{1})\varphi(x)$ and this is the image of $\varphi(x)$ under $\varphi - \lambda_1\mathbb{1}$ and hence $y \in L_1$ again. Therefore the following endomorphism on L_1 is well-defined

$$\varphi_1 : L_1 \to L_1 : x \mapsto \varphi(x)$$

Now, for any $i \in 1\dots r$ let $x_i \neq 0$ be an eigenvector of φ to the eigenvalue λ_i. That is $\varphi(x_i) = \lambda_i x_i$. Then we define $y_i := \varphi(x_i) - \lambda_1 x_i \in L_1$ and claim that y_i is an eigenvector of φ_1 to the eigenvalue λ_i for any $i \in 2\dots r$. This is a simple computation

$$\begin{aligned} y_i &= \varphi(x_i) - \lambda_1 x_i = \lambda_i x_i - \lambda_1 x_i = (\lambda_i - \lambda_1)x_i \\ \varphi_1(y_i) &= \varphi(y_i) = (\lambda_i - \lambda_1)\varphi(x_i) = \lambda_i(\lambda_i - \lambda_1)x_1 = \lambda_i y_i \end{aligned}$$

That is we generally have $\varphi(y_i) = y_i$ and as the λ_i are distinct, we also have $\lambda_i - \lambda_1 \neq 0$ for $i \in 2\dots r$ such that we also have $y_i \neq 0$. This implies $\lambda_i \in \operatorname{Spec}(\varphi_1)$, as we have found the eigenvector y_i. Let us now prove that the minimal polynomial of φ_1 is given to be

$$m_1(t) := (t-\lambda_2)\dots(t-\lambda_r)$$

As we have seen $\lambda_i \in \operatorname{Spec}(\pi_1)$ for any $i \in 2\dots r$ we get $m_{\varphi_1}(\lambda_i) = 0$ by (5.46.(iv)). In particular $(t-\lambda_i) \mid m_{\varphi_1}$ and as these are distinct prime elements of (the PID) $R[t]$ we find $m_1 \mid m_{\varphi_1}$. Conversely consider any $y = \varphi(x) - \lambda_1 x \in L_1$. Then we find

$$\begin{aligned} m_1(\varphi)(y) &= (\varphi-\lambda_2)\dots(\varphi-\lambda_r)(\varphi-\lambda_1)(x) \\ &= (\varphi-\lambda_1)(\varphi-\lambda_2)\dots(\varphi-\lambda_r)(x) \end{aligned}$$

$$= \quad m_\varphi(\varphi)(x) \;=\; 0$$

And as $m_1(\varphi)(y) = 0$ is true for any $y \in L_1$ this is $m_1(\varphi) = 0$. By definition of the minimal polynomial this means $m_{\varphi_1} \mid m_1$ such that together we have $m_{\varphi_1} \approx m_1$. Yet as both polynomials are monic, this is $m_{\varphi_1} = m_1$. In particular the minimal polynomial of φ_1 splits into *distinct* factors

$$m_{\varphi_1}(t) \;:=\; \big(t-\lambda_2\big)\dots\big(t-\lambda_r\big)$$

and as $\dim(L_1) < \dim(M) = n$ we may use the induction hypothesis on φ_1: There is a basis $\{\, u_1,\dots,u_m \,\}$ of L_1 consisting of eigenvectors of φ. As we already know the eigenvalues of φ this means that for any $1 \le i \le m$ we have $\varphi(u_i) = \mu_i$ for some $\mu_i \in \{\, \lambda_2,\dots,\lambda_r \,\}$. Recall that by the dimension formula above we know that $\dim(\mathrm{Eig}_\varphi(\lambda_1)) = n - m$. That is we may choose another basis $\{\, u_{m+1},\dots,u_n \,\}$ of $\mathrm{Eig}_\varphi(\lambda_1)$. In particular we get $\varphi(u_i) = \lambda_i u_i$ for any $m < i \le n$ and hence

$$\{\, u_1,\dots,u_m \,\} \cap \{\, u_{m+1},\dots,u_n \,\} \;=\; \emptyset$$

as any u in the intersection would satisfy $\varphi(u) = \lambda_1 u$ and $\varphi(u) = \lambda_i u$ for some $i \in 2\dots r$. But this is absurd, as $u \neq 0$ (0 never is part of a basis) and $\lambda_1 \neq \lambda_i$. We will now prove that $\{\, u_1,\dots,u_n \,\}$ is linearly independent. That is we assume

$$x \;=\; \sum_{i=1}^{n} a_i u_i \;=\; 0$$

for some $a_i \in R$ and have to verify $a_i = 0$ for all $i \in 1\dots n$. To do this apply $\varphi - \lambda_1 \mathbb{1}$ to x and recall that $\varphi(u_i) = \mu_i u_i$ for $i \le m$ and $\varphi(u_i) = \lambda_1 u_i$ for $i > m$. Using this we compute

$$\begin{aligned}
(\varphi - \lambda_1 \mathbb{1})(x) &= \sum_{i=1}^{n} a_i\big(\varphi(u_i) - \lambda_1 u_i\big) \\
&= \sum_{i=1}^{m} a_i\big(\varphi(u_i) - \lambda_1 u_i\big) \\
&= \sum_{i=1}^{m} a_i\big(\mu_i u_i - \lambda_1 u_i\big) \\
&= \sum_{i=1}^{m} a_i\big(\mu_i - \lambda_1\big) u_i
\end{aligned}$$

As $\{\, u_1,\dots,u_m \,\}$ is linearly independent we find $a_i(\mu_i - \lambda_1) = 0$ for any $i \le m$. But $\mu_i - \lambda_1 \neq 0$ such that this means $a_i = 0$. Thus $x = 0$ has been reduced to $a_{m+1}u_{m+1} + \dots + a_n u_n = 0$ in the first place. And as $\{\, u_{m+1},\dots,u_n \,\}$ is linearly independent, as well, this also means $a_i = 0$ for any $i > m$. Altogether $\{\, u_1,\dots,u_n \,\}$ is a linearly independent subset containing $n = \dim(M)$ elements. By (3.66.(viii)) this means, that $\{\, u_1,\dots,u_n \,\}$ is a basis of M and as any u_i is an eigenvector of φ we have finally arrived at (a).

- The one implication left to prove is (f) $\implies$ (a): But in case of a field R this is a no-brainer: By assumption the dimension of M equals the sum of the dimensions of the eigenspaces $\mathrm{Eig}_\varphi(\lambda_i)$. So for any $i \in 1\dots r$ choose a basis $\mathcal{M}_i \subseteq \mathrm{Eig}_\varphi(\lambda_i)$. In particular $\mathcal{M}_i$ consists of eigenvectors and

by definition $\#\mathcal{M}_i = \mathrm{GM}_\varphi(\lambda_i)$. Now let

$$\mathcal{M} \;:=\; \bigcup_{i=1}^{r} \mathcal{M}_i$$

Then by (5.37.(v)) $\mathcal{M}$ is linearly independent again. And by assumption we have $\#\mathcal{M} = \dim(M)$. Hence by (3.66.(viii)) $\mathcal{M}$ is a basis of M, that consists of eigenvectors of φ and this is (a) already.

□

Proof of (5.49):
By Cayley-Hamilton (5.44.(ii)) we have $c_\varphi(\varphi) = 0$ and hence $m_\varphi \mid c_\varphi$ by property (3) in the definition of the minimal polynomial. But also $m_\varphi(\varphi) = 0$, by property (1), so by the theorem of Fitting (5.48.(iv)) (using $f_k = m_\varphi$ for any $k \in 1 \dots n$) we also have $c_\varphi \mid m_\varphi^n$.
If $p \in R[t]$ is prime such that $p \mid m_\varphi$ then $m_\varphi \mid c_\varphi$ yields $p \mid c_\varphi$, as the divides relation is transitive. Conversely, if $p \mid c_\varphi$ then $c_\varphi \mid m_\varphi^n$ yields $p \mid m_\varphi^n$. But as p is prime, this means $p \mid m_\varphi$, too. □

Proof of (3.92):
First of all it is clear, that is suffices to check the implication (a) $\implies$ (b), due to the symmetry of the equivalence. That is we assume that to top sequence of M's is a complex, resp. an exact chain.
It also suffices to check the case $n = 2$, that is we concern ourselves with the complex $M_0 \to M_1 \to M_2$ and prove that $N_0 \to N_1 \to N_2$ is a complex, respectively its exactness at N_1. For larger chains the arguments can be repeated at any module N_k where $1 \leq k \leq n-1$.
Due to the commutativity of the diagrams we have $\psi_1 = \Phi_1\varphi_1\Phi_0^{-1}$ and $\psi_2 = \Phi_2\varphi_2\Phi_1^{-1}$ respectively. And by assumption that $M_0 \to M_1 \to M_2$ is a complex, we also know $\varphi_2\varphi_1 = 0$. But from this it is easy to see, that also

$$\psi_2\psi_1 \;=\; \Phi_2\varphi_2\Phi_1^{-1}\Phi_1\varphi_1\Phi_0^{-1} \;=\; \Phi_2\varphi_2\varphi_1\Phi_0^{-1} \;=\; \Phi_2 0\Phi_0^{-1} \;=\; 0$$

So let us now assume $M_0 \to M_1 \to M_2$ even is exact, in order to prove the exactness of $N_0 \to N_1 \to N_2$ it suffices to check $\ker(\psi_2) \subseteq \operatorname{im}(\psi_1)$, as the converse inclusion has just been shown. Thus consider any $n_1 \in \ker(\psi_2) \subseteq N_1$ and let $m_1 := \Phi_1^{-1}(n_1)$. Then we find

$$\varphi_2(m_1) \;=\; \Phi_2^{-1}\psi_2\Phi_1(m_1) \;=\; \Phi_2^{-1}\psi_2(n_1) \;=\; \Phi_2^{-1}(0) \;=\; 0$$

That is $m_1 \in \ker(\varphi_2) = \operatorname{im}(\varphi_1)$ and hecne there is some $m_0 \in M_0$ such that $\varphi_1(m_0) = m_1$. Now let $n_0 := \Phi_0(m_0)$ then we conversely find

$$\psi_1(n_0) \;=\; \Phi_1\varphi_1\Phi_0^{-1}(n_0) \;=\; \Phi_1\varphi_1(m_0) \;=\; \Phi_1(m_1) \;=\; n_1$$

That is $n_1 \in \operatorname{im}(\psi_1)$ and as n_1 has been chosen arbitrarily we have truly established $\ker(\psi_2) \subseteq \operatorname{im}(\psi_1)$ as claimed. □

Proof of (3.93):
In order to prove the left-exactness of the push-forward we have to check two things: φ_* is injective and $\operatorname{im}(\varphi_*) = \ker(\psi_*)$. The injectivity is easy however: suppose $\varphi f_1 = \varphi f_2$ for some homomorphisms f_1, $f_2 \in \mathcal{L}(M, U)$. That is for any $m \in M$ we get $\varphi f_1(m) = \varphi f_2(m)$, but as φ is injective by assumption this means $f_1(m) = f_2(m)$ and hence $f_1 = f_2$, since $m \in M$ has been arbitrary. Also the inclusion

$\mathrm{im}(\varphi_*) \subseteq \mathrm{kn}(\psi_*)$ is easy: By assumption we have $\mathrm{im}(\varphi) = \mathrm{kn}(\psi)$ and hence $\psi\varphi = 0$. So if we start with some $f \in \mathcal{L}(M,U)$ and compute $\psi_*(\varphi_*(f)) = \psi\varphi f = 0f = 0$ we truly find $\varphi_*(f) \in \mathrm{kn}(\psi_*)$. Finally for $\mathrm{kn}(\psi_*) \subseteq \mathrm{im}(\varphi_*)$ we are given some $g \in \mathcal{L}(M,V)$ such that $\psi g = 0$ and need to find some $f \in \mathcal{L}(M,U)$ such that $\varphi f = g$. But $\psi g = 0$ is just $\mathrm{im}(g) \subseteq \mathrm{kn}(\psi) = \mathrm{im}(\varphi)$ again and hence the map $f = \varphi^{-1}g$ is well-defined, since φ is injective.
In order to prove the left-exactness of the pull-back we have to check two things: ψ^* is injective and $\mathrm{im}(\psi^*) = \mathrm{kn}(\varphi^*)$. The injectivity is easy however: suppose $h_1\psi = h_2\psi$ for some homomorphisms h_1, $h_2 \in \mathcal{L}(W,M)$. Since ψ is surjective by assumption, for any $w \in W$ there is some $v \in V$ such that $\psi(v) = w$. And using this we can compute

$$h_1(w) \;=\; h_1\psi(v) \;=\; h_2\psi(v) \;=\; h_2(w)$$

And since w has been arbitrary this means $h_1 = h_2$. The inclusion $\mathrm{im}(\psi^*) \subseteq \mathrm{kn}(\varphi^*)$ is easy as well: We have $\mathrm{im}(\varphi) = \mathrm{kn}(\psi)$ by assumption and in particular $\psi\varphi = 0$. Thus for any $h \in \mathcal{L}(W,M)$ we get $\varphi^*(\psi^*(h)) = h\psi\varphi = h0 = 0$. Finally for $\mathrm{kn}(\varphi^*) \subseteq \mathrm{im}(\psi^*)$ we are given some $g \in \mathcal{L}(V,M)$ such that $g\varphi = 0$ and need to find some $h \in \mathcal{L}(W,M)$ such that $g = h\psi$. But this h can be defined explicitly: given any $w \in W$ choose some $v \in V$ such that $\psi(v) = w$ [which is possible, since ψ is surjective] and let

$$h(w) \;:=\; g(v)$$

Of course we need to check the well-definedness of h, that is consider any two v_1 and $v_2 \in V$ such that $\psi(v_1) = \psi(v_2)$. That is $v_2 - v_1 \in \mathrm{kn}(\psi) = \mathrm{im}(\varphi)$ and hence there is some $u \in U$ such that $\varphi(u) = v_2 - v_1$. In other words $v_2 = v_1 + \varphi(u)$ and thereby we find

$$g(v_2) \;=\; g(v_1 + \varphi(u)) \;=\; g(v_1) + g\varphi(u) \;=\; g(v_1) + 0$$

We also need to check, that $h : W \to M$ is R-linear. But if $v \in V$ satisfies $\psi(v) = w$, then clearly $\psi(av) = a\psi(v) = aw$ and hence $h(aw) = g(av) = ag(v) = ah(w)$. Likewise for $\psi(v_k) = w_k$ we see $\psi(v_1 + v_2) = \psi(v_1) + \psi(v_2) = w_1 + w_2$ and hence $h(w_1 + w_2) = g(v_1 + v_2) = g(v_1) + g(v_2) = h(w_1) + h(w_2)$. Hence we have found our $h \in \mathcal{L}(W,M)$ that satisfies $\psi^*(h) = h\psi = g$. □

Proof of (3.94):
It suffices to check the case $n = 2$, that is we concern ourselves with the chain $M_0 \to M_1 \to M_2$ and prove its exactness at M_1. For larger chains the arguments can be repeated at any module M_k where $1 \leq k \leq n-1$.

(i) First of all take $L = M_0$, by assumption we have $0 = (\varphi_2)_*(\varphi_1)_*(\mathbb{1}) = \varphi_2\varphi_1$ and hence $\mathrm{im}(\varphi_1) \subseteq \mathrm{kn}(\varphi_2)$. For the converse inclusion regard $L = \mathrm{kn}(\varphi_2)$ and the inclusion $\iota : L \to M_1 : k \mapsto k$. Then, as k is in the kernel of φ_2 we find $(\varphi_2)_*(\iota)(k) = \varphi_2\iota(k) = \varphi_2(k) = 0$ and hence $(\varphi_2)_*(\iota) = 0$. But since $\iota \in \mathrm{kn}((\varphi_2)_*) = \mathrm{im}((\varphi_1)_*)$ there has to be some $\alpha \in \mathcal{L}(L, M_0)$ such that $\iota = (\varphi_1)_*(\alpha) = \varphi_1\alpha$. If we now take any $k \in L = \mathrm{kn}(\varphi_2)$ then this means $k = \iota(k) = \varphi_1\alpha(k) \in \mathrm{im}(\varphi_1)$. Thus we have also established $\mathrm{kn}(\varphi_2) \subseteq \mathrm{im}(\varphi_1)$.

(ii) Now take $N = M_2$, by assumption we have $0 = (\varphi_1)^*(\varphi_2)^*(\mathbb{1}) = \varphi_2\varphi_1$ and hence $\mathrm{im}(\varphi_1) \subseteq \mathrm{kn}(\varphi_2)$ again. For the converse inclusion regard $N = M_1/\mathrm{im}(\varphi_1)$ and $\varrho : M_1 \to N : y \mapsto y + \mathrm{im}(\varphi_1)$ the canonocal epimorphism. Then for any $x \in M_0$ we find $(\varphi_1)^*(\varrho)(x) = \varrho\varphi_1(x) =$

$\varphi_1(x) + \mathrm{im}(\varphi_1) = 0$ and hence $(\varphi_1)^*(\varrho) = 0$ which is $\varrho \in \mathrm{kn}((\varphi_1)^*) = \mathrm{im}((\varphi_2)^*)$ by assumption, again. That is there is some $\gamma \in \mathcal{L}(M_2, N)$ such that $\varrho = (\varphi_2)^*(\gamma) = \gamma\varphi_2$. Thus if $k \in \mathrm{kn}(\varphi_2)$, then $k + \mathrm{im}(\varphi_1) = \varrho(k) = \gamma\varphi_2(k) = \gamma(0) = 0$ such that $k \in \mathrm{im}(\varphi_1)$. Thus we have also established $\mathrm{kn}(\varphi_2) \subseteq \mathrm{im}(\varphi_1)$.

□

Proof of (3.45):

(i) Suppose $M \neq 0$, as M is finitely generated, the sub-module $0 \leq_{\mathfrak{m}} M$ is cofinite. Hence by (3.18) there is a maximal sub-module $Q \leq_{\mathfrak{m}} M$ such that $P \subseteq Q \subset M$. As Q is maximal, M/Q is a non-zero, simple R-module [$M/Q \neq 0$, as $Q \neq M$ and by the correspondence theorem (3.16.(ii)): consider a sub-module $U/Q \leq_{\mathfrak{m}} M/Q$, then $U \leq_{\mathfrak{m}} M$ satisfies $Q \subseteq U \subseteq M$ and hence $Q = U$ or $U = M$ due to the maximality of Q]. Therefore

$$\mathfrak{m} := \mathrm{ann}_R\left(M \big/ Q\right)$$

is a maximal ideal $\mathfrak{m} \in \mathrm{Smax}(R)$, according to (3.24.(i)). By definition of $\mathfrak{m}$ we have $ax + Q = a(x + Q) = 0 + Q$ for any $a \in \mathfrak{m}$ and $x \in M$. That is $ax \in Q$ and hence $\mathfrak{m}M \subseteq Q$. Now by assumption we get $Q \subseteq M = \mathfrak{m}M \subseteq Q$. But that is $Q = M$ in contradiction to $Q \neq M$, such that the assumption $M \neq 0$ must have been false.

(ii) By (3.40.(v)) we know that $\mathfrak{m}(M/P)$ equals $(\mathfrak{m}M + P)/P$ and hence we have the following identities (by the assumptions on P)

$$\mathfrak{m}\left(M \big/ P\right) = \mathfrak{m}M + P \big/ P = M \big/ P$$

for any maximal ideal $\mathfrak{m} \trianglelefteq_{\mathfrak{i}} R$. Yet as P is cofinite the quotient module M/P is finitely generated. Hence we may use (i) to find $M/P = 0$ and this is nothing but $M = P$.

(iii) If φ is surjective, then $\varphi/\mathfrak{m}$ is surjective for any ideal $\mathfrak{m} \subseteq R$, as we have seen in (3.40.(vii)). Conversely if $\varphi/\mathfrak{m}$ is surjective, then for any $y \in N$ there is some $x \in M$ such that $\varphi(x) + \mathfrak{m}N = y + \mathcal{M}N$. That is there is some $z \in \mathfrak{m}N$ such that $y = \varphi(x) + z \in \mathrm{im}(\varphi) + \mathfrak{m}N$. And as $y \in N$ has been arbitrary, this means $N = \mathrm{im}(\varphi) + \mathfrak{m}N$. As $\mathrm{im}(\varphi)$ is cofinite and this is tru for any maximal ideal $\mathfrak{m}$, we may invoke (ii) to find $\mathrm{im}(\varphi) = N$, but this is nothing but the surjectivity of φ.

(iv) If φ is bijective, then $\varphi/\mathfrak{m}$ is bijective for any ideal $\mathfrak{m} \subseteq R$, as we have seen in (3.40.(vii)). Conversely: as M is finitely generated, the zero-module $0 \leq_{\mathfrak{m}} M$ is cofinite and hence also $\mathrm{im}(\varphi) \leq_{\mathfrak{m}} M$ is cofinite. So by (iii) we already know, that φ is surjective, as the $\varphi/\mathfrak{m}$ are surjective (even bijective). But a surjective endomorphism of a finitely generated R-module is bijective by (5.44).

□

Proof of (3.83):

(i) Suppose I and J have the same cardinality, by definition this means, that there is a bijection $\sigma : I \to J$. And by construction $M := R^{\oplus I}$ has the canoncial basis $e_k = (\delta_{i,k}) \in M$, where $k \in I$.

That is the k-th component of e_k is 1, all others ($i \neq k$) are 0. Likewise we denote the canonical basis of $N := R^{\oplus J}$ by $f_l = (\delta_{j,l}) \in N$, where $l \in J$. This clearly gives rise to a well-defined homomorphism of R-modules:

$$\varphi \ : \ M \to N \ : \ \sum_{i \in I} a_i e_i \mapsto \sum_{i \in I} a_i f_{\sigma(i)}$$

As σ is surjective and $\left\{ f_j \mid j \in J \right\}$ generates N we see that Φ is surjective. Suppose $\Phi(a_i) = 0$, as σ is injective and $\left\{ f_j \mid j \in J \right\}$ is R-linearly independent this means that $a_i = 0$ for any $i \in I$. This is $\mathrm{kn}(\Phi) = 0$ and hence Φ also is injective. Altogether Φ is an isomorphism.

It remains to prove the converse implication, that is we suppose that $M := R^{\oplus I}$ and $N := R^{\oplus J}$ are isomorphic. As R is a non-zero, commutative ring we may use (2.4.(ii)) to pick up a maximal ideal $\mathfrak{m} \trianglelefteq_{\mathrm{i}} R$ of R (containing $0 \subset R$). Then, as $\mathfrak{m}$ is maximal, $F := R/\mathfrak{m}$ is a field.

As we have seen in (3.41) the quotient $M/\mathfrak{m}M$ is isomorphic to $F^{\oplus I}$, by virtue of the following isomorphism

$$F^{\oplus I} \xrightarrow{\sim} R^{\oplus I} \Big/ \mathfrak{m}R^{\oplus I} \ : \ (b_i + \mathfrak{m}) \mapsto (b_i) + \mathfrak{m}R^{\oplus I}$$

In complete analogy we find an isomorphism of F-vector-spaces between $F^{\oplus J}$ and the quotient $N/\mathfrak{m}N$. Now, as $M \cong_{\mathfrak{m}} N$ are isomorphic (by assumption), so are the quotient modules $M/\mathfrak{m}M \cong_{\mathfrak{m}} N/\mathfrak{m}N$, by virtue of (3.40.(vii)). And therefore we find a chain of isomorphies of F-vector-spaces connecting

$$F^{\oplus I} \ \cong_{\mathfrak{m}} \ R^{\oplus I} \Big/ \mathfrak{m}R^{\oplus I} \ \cong_{\mathfrak{m}} \ R^{\oplus J} \Big/ \mathfrak{m}R^{\oplus J} \ \cong_{\mathfrak{m}} \ F^{\oplus J}$$

Clearly isomorphic modules have the same dimension (the isomorphism transfers bases). And as $F^{\oplus I}$ has dimension $|I|$ (using the canonical basis) altogether we find

$$|I| \ = \ \dim(F^{\oplus I}) \ = \ \dim(F^{\oplus J}) \ = \ |J|$$

(ii) Let $\Phi : R/\mathfrak{a} \to R/\mathfrak{b}$ be the isomorphism of R-modules, that we assumed to exist. Further let $v + \mathfrak{b} := \Phi(1 + \mathfrak{a})$ and $u + \mathfrak{a} := \Phi^{-1}(1 + \mathfrak{b})$. Then - as Φ is R-linear - we get

$$\Phi(uv + \mathfrak{a}) \ = \ v\Phi(u + \mathfrak{a}) \ = \ v(1 + \mathfrak{b}) \ = \ v + \mathfrak{b} \ = \ \Phi(1 + \mathfrak{a})$$

As Φ is invertible this implies $uv + \mathfrak{a} = 1 + \mathfrak{a}$ and hence $u + \mathfrak{a} = (v + \mathfrak{a})^{-1} \in (R/\mathfrak{a})^*$ is invertible. Now consider any $a \in R$, then $a \in \mathfrak{a}$ is equivalent to $a + \mathfrak{a} = 0 + \mathfrak{a}$. And as $u + \mathfrak{a}$ is a unit this is equivalent to $ua + \mathfrak{a} = 0 + \mathfrak{a}$. Now compute

$$0 + \mathfrak{b} \ = \ \Phi(0 + \mathfrak{a}) \ = \ \Phi(ua + \mathfrak{a}) \ = \ a\Phi(u + \mathfrak{a}) \ = \ a(1 + \mathfrak{b}) \ = \ a + \mathfrak{b}$$

That is $a + \mathfrak{a} = 0 + \mathfrak{a}$ is equivalent to $a + \mathfrak{b} = 0 + \mathfrak{b}$. Therefore $a \in \mathfrak{a}$ is equivalent to $a \in \mathfrak{b}$ and this is just the equality $\mathfrak{a} = \mathfrak{b}$ of subsets of R.

□

Proof of (3.95):

(i) It has already been shown in section 2.7 that $\mathbb{Z}$ is a PID. It only remains to verify, that $\mathbb{P}$ is infinite. Hence we suppose, that $\mathbb{P}$ is finite, say $\mathbb{P} = \{ p_1, \ldots, p_n \}$. Then we let $b := p_1 \cdot \cdots \cdot p_n + 1 \in \mathbb{Z}$ and choose an arbitrary prime divisor $p \geq 0$ of b, that is $b = ap$ for some $a \in \mathbb{Z}$. As $\mathbb{P}$ encompasses *all* (positive) prime elements of $\mathbb{Z}$ there is some $i \in 1 \ldots n$ with $p = p_i$. Without loss of generality we may take $p = p_1$. Now

$$p_1 \cdot \cdots \cdot p_n + 1 \;=\; b \;=\; ap \;=\; ap_1$$

Hence $1 = p_1(a - p_2 \cdot \cdots \cdot p_n)$ which means that p_1 is a unit of $\mathbb{Z}$ - an obvious contradiction to being a prime element. Hence $\mathbb{P}$ is not finite.

(ii) Suppose $\mathbb{Q} = \mathrm{Lh}(x_1, \ldots, x_n)$ was finitely generated, where $x_i = a_i/b_i$. Then we choose a prime number $p \in \mathbb{P}$ such that for any $i \in 1 \ldots n$ we have $p \not| \; b_i$. Such a prime exists, as by (i) there are infinitely many primes and all the b_i are only divisible by finitley many primes. Now suppose $1/p = k_1 x_1 + \cdots + k_n x_n$ for some $k_i \in \mathbb{Z}$. Let $b := b_1 \cdot \cdots \cdot b_n$ and $\widehat{b}_i := b/b_i \in \mathbb{Z}$, then

$$\frac{1}{p} \;=\; \sum_{i=1}^{n} k_i \frac{a_i}{b_i} \;=\; \frac{1}{b} \sum_{i=1}^{n} k_i a_i \widehat{b}_i \quad \Longrightarrow \quad b \;=\; p \sum_{i=1}^{n} k_i a_i \widehat{b}_i$$

In particular p would divide b and hence some of the b_i (as p is prime) in contradiction to the choice of p. Hence there can be no finite generating set of $\mathbb{Q}$ as an $\mathbb{Z}$-module.

It remains to show, that the set P truly generates $\mathbb{Q}$. To do this consider any $x = a/b \in \mathbb{Q}$ and write down a primary decomposition

$$b \;=\; s p_1^{k(1)} \cdot \cdots \cdot p_n^{k(n)}$$

where $s = 1$ or $s = -1$ and $p_i \in \mathbb{P}$. We will now use induction on the number n of distinct prime factors of b. If $n = 0$ then we readily have $x = a/s = as \in \mathbb{Z}$. And if $n = 1$ then

$$x \;=\; as \frac{1}{p_1^{k(1)}} \;\subseteq\; \mathbb{Z} \frac{1}{p_1^{k(1)}} \;\in\; \mathrm{Lh}(P)$$

For the induction step $n - 1 \to n$ let us abbreviate $q := p_1^{k(1)} \cdot \cdots \cdot p_{n-1}^{k(n-1)}$ and $p := p_n^{k(n)}$. Then $x = a/(sqp) = (as)/(qp)$. As p and q are relatively prime $\gcd(p, q) = \pm 1$ and $\mathbb{Z}$ is a PID there are some u and $v \in \mathbb{Z}$ such that $uq + vp = as$. Hence we find (note that $u/p \in \mathrm{Lh}(\mathbb{P})$ as in the case $n = 1$ and $v/q \in \mathrm{Lh}(\mathbb{P})$ by induction hypothesis)

$$x \;=\; \frac{as}{qp} \;=\; \frac{uq + vp}{qp} \;=\; \frac{u}{p} + \frac{v}{q} \;\in\; \mathrm{Lh}(\mathbb{P}) + \mathrm{Lh}(\mathbb{P}) \;=\; \mathrm{Lh}(\mathbb{P})$$

□

Proof of (3.49):

(i) First suppose M is simple and consider any $0 \neq x \in M$, then we need to show that $M = Rx$. But as $Rx \;\leq_{\mathsf{m}}\; M$ is a sub-module and M is simple we necessarily have $Rx = 0$ or $Rx = M$. But as also $0 \neq x \in Rx$ this only leaves $Rx = M$. For the converse direction we need to show that

M is simple, that is we pick up some sub-module $P \leq_{\mathfrak{m}} M$ and have to show $P = 0$ or $P = M$. If $P \neq 0$, then there is some $x \in P$ with $x \neq 0$. For this x we then get $M = Rx \subseteq P \subseteq M$ by assumption, such that truly $P = M$.

(ii) Here we have $M = Rm$, but in (3.22.(ii)) we have proved the following isomorphy of R-modules

$$\Phi \; : \; {}^{R}\Big/_{\mathsf{ann}(m)} \; \cong_{\mathfrak{m}} \; M \; : \; a + \mathsf{ann}(m) \mapsto am$$

Hence M is simple if and only if $R/\mathsf{ann}(m)$ is such. But by the correspondence theorem of sub-modules (3.16.(ii)) the sub-modules of $R/\mathsf{ann}(m)$ are of the form $P/\mathsf{ann}(m)$ for some sub-module $P \leq_{\mathfrak{m}} R$ with $\mathsf{ann}(m) \subseteq P$. That is: if $Q \leq_{\mathfrak{m}} M$ is a sub-module of M, then $\Phi^{-1}(Q) = P/\mathsf{ann}(m)$ for some $P \leq_{\mathfrak{m}} R$ and vice versa. Thereby $0 \leq_{\mathfrak{m}} M$ corresponds to $\mathsf{ann}(m) \leq_{\mathfrak{m}} R$ and $M \leq_{\mathfrak{m}} M$ corresponds to $R \leq_{\mathfrak{m}} R$. Any other sub-module (on either side) would spoil the simplicity and would correspond to some sub-module on the other side.

(v) Consider some module-homomorphism $\varphi : M \to N$. If $\varphi = 0$ then there is nothing ot prove, so let us consider $\varphi \neq 0$. As $\mathsf{kn}(\varphi) \leq_{\mathfrak{m}} M$ is a sub-module, but M is simple, we either have $\mathsf{kn}(\varphi) = 0$ or $\mathsf{kn}(\varphi) = M$. But $\varphi \neq 0$ rules out $\mathsf{kn}(\varphi) = M$ which leaves $\mathsf{kn}(\varphi) = 0$, which again is the injectivity of φ. Likewise, as $\mathsf{im}(\varphi) \leq_{\mathfrak{m}} N$ is a sub-module, but N is simple as well, we have $\mathsf{im}(\varphi) = 0$ or $\mathsf{im}(\varphi) = N$. Again $\varphi \neq 0$ rules out $\mathsf{im}(\varphi) = 0$ which leaves $\mathsf{im}(\varphi) = N$, which also is the surjectivity of φ.

(vi) By (v) we have $\mathsf{mend}(M) = \mathsf{maut}(M) \cup \{0\}$ as any non-zero endomorphism $\varphi : M \to M$ already is bijective. That is for any $\varphi \in \mathsf{mend}(M)$ there is some $\varphi^{-1} \in \mathsf{mend}(M)$ with $\varphi\varphi^{-1} = \mathbb{1}$ and $\varphi^{-1}\varphi = \mathbb{1}$. That is any φ is invertible. Hence the *ring* $\mathsf{mend}(M)$ (using the composition as multiplication) is a *division ring*.

(iii) As M is simple, then (i) implies $Rx = M = Ry$. Hence using the same reasoning as in (ii) we find two isomorphisms of R-modules

$$\Phi \; : \; {}^{R}\Big/_{\mathsf{ann}(x)} \; \cong_{\mathfrak{m}} \; M \; : \; a + \mathsf{ann}(x) \mapsto ax$$

$$\Psi \; : \; {}^{R}\Big/_{\mathsf{ann}(y)} \; \cong_{\mathfrak{m}} \; M \; : \; b + \mathsf{ann}(y) \mapsto by$$

Composing $\Psi^{-1}\Phi : R/\mathsf{ann}(x) \to R/\mathsf{ann}(y)$ we find an isomorphism of R-modules (defined by $a + \mathsf{ann}(x) \mapsto b + \mathsf{ann}(y)$ where $ax = by$). however by (3.83.(ii)) we know that this implies $\mathsf{ann}(x) = \mathsf{ann}(y)$ already. And the maximality of $\mathsf{ann}(y)$ has already been proved in (ii) (as in a commutative ring any sub-module already is an ideal).

(iv) If M is simple, then by (i) M alredy is of the form $M = Rx$ as $x \neq 0$. That is we find some $a \in R$ such that $y = ax$ since $y \in M = Rx$. As R is a commutative ring, we get an R-module-endomorphism by letting

$$\mu_a \; : \; M \to M \; : \; x \mapsto ax$$

As M is simple (vi) implies that we either have $\mu_a = 0$ or μ_a is bijective. But as $\mu_a(x) = ax = y \neq 0$ this rules out $\mu_a = 0$ such that μ_a truly is an an R-module-automorphism.

(vii) Fix some $0 \neq m \in M$, then as M is simple, we have $M = Rm$ according to (i). As $\varphi(m) \in M = Rm$ again, there is some $a \in R$ such that $\varphi(m) = am$. And for any $b \in R$ we then compute $\varphi(bm) = b\varphi(m) = b(am) = (ba)m = (ab)m = a(bm)$ as R is commutative. And as $M = Rm$ this means $\varphi(x) = ax$ for any $x \in M$. That is $\varphi = \mu_a : x \mapsto ax$ as has been claimed.

□

Proof of (3.51):

(i) Clearly, if xe and $ye \in Ae$ then $xe + ye = (x + y)e \in Ae$ and $(xe)(ye) = (xey)e \in Ae$ again (we even have $(xe)(ye) = x(ey)e = x(ye)e = xye^2 = xye$). Also for any $a \in R$ we have $a(xe) = (ax)e \in Ae$ such that Ae is an R-sub-semi-algebra of Ae. Also if $z \in A$ then $z(xe) = (zx)e \in Ae$ and $(xe)z = x(ez) = x(ze) = (xz)e \in Ae$ such that Ae also is an ideal of A. It remains to prove $1_{Ae} = e$ that is for any $xe \in Ae$ we need to show $e(xe) = xe$ and $(xe)e = xe$. The latter is due to $(xe)e = xe^2 = xe$ however and the first follows from $e(xe) = e(ex) = e^2x = ex = xe$, as well.

(ii) Clearly $0 \in \mathrm{cen}(A)$ as for any $g \in A$ we have $0g = 0 = g0$ and if $a \in R$, f, $f' \in \mathrm{cen}(A)$ then we get $(af)g = a(fg) = f(ag) = (ag)f = a(gf) = g(af)$ and $(f + f')g = fg + f'g = gf + gf' = g(f + f')$ such that af and $f + f' \in \mathrm{cen}(A)$ again. So far we have shown that $\mathrm{cen}(A) \leq_{\mathsf{m}} A$ is an R-sub-module of A. But also $(ff')g = f(f'g) = f(gf') = (fg)f' = (gf)f' = g(ff')$ implies $ff' \in \mathrm{cen}(A)$ as well. Altogether $\mathrm{cen}(A) \leq_{\mathsf{b}} A$ and if $1 \in A$ is the unit element then $1g = g = g1$ for any $g \in A$ such that $1 \in \mathrm{cen}(A)$ again. In particular, if u and $v \in \mathrm{cen}(A)$ then for any $g \in A$ we also get $g(uv) = (gu)v = (ug)v = u(gv) = u(vg) = (uv)g$ such that $uv \in \mathrm{cen}(A)$ again. So we also found that $\mathrm{cen}(A)$ is multiplicatively closed.

(iii) First of all we have $e(1 - e) = e - e^2 = e - e = 0$ and $(1 - e)e = e - e^2 = 0$ since e is idempotent, such that $e \perp (1 - e)$. Also we get $(1 - e)^2 = 1 - 2e + e^2 = 1 - 2e + e = 1 - e$ such that $1 - e$ is idempotent again. If $e \in \mathrm{cen}(A)$ also is central, then for any $x \in A$ we also get $x(1 - e) = x - xe = x - ex = (1 - e)x$ such that $1 - e \in \mathrm{cen}(A)$ is central, as well.

□

Proof of (3.52):

(i) Clearly for any $x \in A$ assumption (1) yields the equality $x = x1_A = x(\sum_i e_i) = \sum_i (xe_i) \subseteq \sum_i Ae_i$. And as x has been arbitrary this is $A = \sum_i Ae_i$. It remains to verify that for any $j \in 1 \ldots n$ we have

$$Ae_j \cap \left(\sum_{i \neq j} Ae_i \right) \;=\; 0$$

Thus consider any $x \in Ae_j$ that is $x = x_j e_j$ for some $x_j \in A$. Then we get $xe_j = x_j e_j e_j = x_j e_j = x$ by assumption (2). If now $x \in \sum_{i \neq j} Ae_i$ say $x = \sum_{i \neq j} x_i e_i$ then by assumption (3) we also get $x = xe_j = (\sum_{i \neq j} x_i e_i)e_j = \sum_{i \neq j} x_i e_i e_j = \sum_{i \neq j} x_i 0 = 0$. That is $x = 0$ as claimed.

(ii) The A-linearity of P_i is obvious: if x, $y \in A$ then $P_i(xy) = (xy)e_i = x(ye_i) = xP_i(y)$ and $P_i(x + y) = (x + y)e_i = xe_i + ye_i = P_i(x) + P_i(y)$. And the multiplicativity is due to the fact that e_i is a central idempotent: $P_i(xy) = (xy)e_i = (xy)e_i^2 = x(ye_i)e_i = x(e_i y)e_i = (xe_i)(ye_i) = P_i(x)P_i(y)$.

And finally we have $P_i(1) = e_i$ where $e_i \in Ae_i$ is the unit element of Ae_i, as $(xe_i)e_i = xe_i^2 = xe_i$ and $e_i(xe_i) = (e_ix)e_i = (xe_i)e_i = xe_i$. So altogether P_i truly is a homomorphism of A-algebras. The surjectivity of P_i is trivial, so it only remains to prove the equality for the kernel. Let $x = \sum_j x_j e_j$ then

$$P_i(x) \;=\; \sum_{j=1}^{n} P_i(x_j e_j) \;=\; \sum_{j=1}^{n} x_j e_j e_i \;=\; \sum_{j=1}^{n} x_j \delta_{i,j} e_j \;=\; x_i e_i$$

Hence we have $x \in \mathrm{kn}(P_i)$ if and only if $0 = P_i(x) = x_i e_i$ and considering that $x = \sum_j x_j e_j$ this is equivalent to $x = \sum_{j\neq i} x_j e_j$ that is to $x \in \sum_{j\neq i} Ae_j$. Note however that x_i itself need *not* be zero, it is the product $x_i e_i$ only, that has to be zero.

Let us denote $P := P_1 \oplus \cdots \oplus P_n : A \to A_1 \oplus \cdots \oplus A_n$ which is defined by $P(x) = (xe_1, \ldots, xe_n)$, that is P is the map of which we claim that it is an isomorphism of A-algebras. But as any P_i is a homomorphism of A-algebras it is clear, by construction, that P is an A-algebra-homomorphism again. And the bijectivity is due to (i), the inverse map is given by $(x_i) \mapsto x_1 + \cdots + x_n$.

(iii) Let us denote the basis of A by $\{ f_i \mid i \in I \}$. Then $1_A \in A$ has a basis representation concerning this basis

$$1_A \;=\; \sum_{i\in I} u_i f_i$$

where only finitely many of the $u_i \in R$ are non-zero. As also $f_i f_j \in A$ there are some $a_{i,j,k} \in R$ such that $f_i f_j$ has the basis representation

$$f_i f_j \;=\; \sum_{k\in I} a_{i,j,k} f_k$$

Combining these we find $f_j = 1_A f_j = (\sum_i u_i f_i) f_j = \sum_i u_i f_i f_j = \sum_i u_i \sum_k a_{i,j,k} f_k = \sum_k (\sum_i u_i a_{i,j,k}) f_k$. Comparing coefficients we find that for any $j, k \in I$ we get

$$\sum_{i\in I} u_i a_{i,j,k} \;=\; \delta_{j,k}$$

Now fix an arbitrary $r \in I$ and define $\kappa : A \to R$ by linear expansion of $f_i \mapsto a_{i,r,r}$ then for any $a \in R$ we can compute

$$\kappa(a1_A) = \kappa\left(a \sum_{i\in I} u_i f_i\right) = a \sum_{i\in I} u_i a_{i,r,r} = a \sum_{i\in I} u_i a_{i,r,r} = a$$

That is $\kappa\iota(a) = \kappa(a1_A) = a$ such that $\kappa\iota = \mathbb{1}_R$ and in particular ι is injective (and κ is surjective). Now let $A' := \mathrm{kn}(\kappa) \;\leq_{\mathfrak{m}}\; A$ and consider an arbitrary $x \in A$. Let $a := \kappa(x)$ and $x' := x - a1_A$ then $\kappa(x') = \kappa(x) - \kappa(a1_A) = a - a = 0$ such that $x' \in A'$. Thereby we have $x = a1_A + x'$ such that $A = R1_A + A'$. It remains to verify $(R1_A) \cap A' = 0$. Hence consider some $x \in (R1_A) \cap A'$ say $x = a1_A$. Then $0 = \kappa(x) = \kappa(a1_A) = a$ such that from $x = 0$ we get $A = R1_A \oplus A'$ as claimed.

□

Proof of (3.54):

(i) (a) $\implies$ (b): consider some idempotents $e, f \in A$ with $e \perp f$ (that is $ef = 0 = fe$) and $e + f = 1$.

Then all requirements of (3.52.(i)) are satisfied, such that we get the decoposition $A = Ae \oplus Af$ where the direct sum is that of A-modules. But by assumption A is indecomposable as an A-module such that $Ae = 0$ or $Af = 0$. But as $1 \in A$ this implies $e = 0$ or $f = 0$, as claimed.

(b) $\implies$ (c): it is clear that $0^2 = 0$ and $1^2 = 1$, conversely consider an idempotent $e \in A$ then we need to show $e = 0$ or $e = 1$. To do this let $f := 1 - e$, then $e + f = 1$ is clear and $e \perp f$ is due to (3.51.(iii)). So by assumption we get $e = 0$ or $f = 0$. The case $f = 0$ already is $e = 1$ however.

(c) $\implies$ (a): suppose $A = P \oplus Q$ is the direct sum of some A-sub-modules $P, Q \leq_{\mathsf{m}} A$. Then there are some $p \in P$ and $q \in Q$ such that $1 = p + q$. Now compute $p = p1 = p(p + q) = p^2 + pq$. As Q is an A-sub-module of A we have $pq \in Q$, but also $pq = p - p^2 \in P$ such that $pq \in P \cap Q = \{0\}$ which is $pq = 0$. This also proves $p^2 = p$ such that $p \in \mathrm{IP}(A)$ is an idempotent. But by assumption this means $p = 0$ or $p = 1$. In complete analogy we find $q = 0$ or $q = 1$. If we had $p = 1$ and $q = 1$ then $1 = p + q = 1 + 1$ such that $0 = 1$ in contradiction to $A \neq 0$. So we have $p = 0$ or $q = 0$. Now for any $x \in A$ we get $x = x1 = x(p + q) = xp + xq$ where $xp \in P$ as $p \in P$ and P is an A-sub-module of A. Likewise $xq \in Q$. Let us first regard the case $p = 0$: then for any $x \in A$ this would imply $x = xq \in Q$ such that $Q = A$. But as $A = P \oplus Q$ this means $P = 0$. In complete analogy $q = 0$ yields $Q = 0$ such that we have established the indecomposability of A.

(ii) (a) $\implies$ (d): let us consider some $e, f \in \mathrm{CIP}(A)$ such that $1 = e + f$, that is $ef = 0$ and $e + f = 1$. Then we take to the A-sub-semi-algebras $U := Ae$ and $U := Af$. Note that U and V thereby also are unital R-sub-semi-algebras of A according to (3.51.(i)). And clearly we have the following isomorphy of R-algebras

$$A \xrightarrow{\sim} U \oplus V \ : \ x \mapsto (xe, xf)$$

according to (3.52.(ii)). By assumption (a) this implies $U = 0$ or $V = 0$ such that $e = 0$ or $f = 0$, which is (d).

(c) $\iff$ (d): If $1 \in A$ is simple, then $A = A1$ trivially is a block. Conversely suppose we had $A = As$ for some simple element $s \in A$. Then there is some $r \in A$ such that $1 = rs$. And as s is central, this also is $sr = 1$ such that $s \in A^*$ is a unit element. Due to the isomorphy $A \xrightarrow{\sim} As : x \mapsto xs$ it is clear that $1 \in A$ has to be simple as well, as it corresponds to the simple element $s \in As = A$.

(d) $\implies$ (e): clearly $0, 1 \in A$ are central idempotents, so conversely let us assume we are given some $e \in \mathrm{CIP}(A)$. Then we need to show $e = 0$ or $e = 1$. But according to (3.51.(iii)) $f := 1 - e \in \mathrm{CIP}(A)$ is a central idempotent again, with $e \perp f$. Hence $1 = e \oplus f$ which implies $e = 0$ or $f = 0$, since 1 was assumed to be simple. But thereby $f = 0$ is just $e = 1$ again.

(e) $\implies$ (a): Suppose we had a decomposition $\Phi : A \xrightarrow{\sim} U \oplus V$ into some R-algebras U and V, that is Φ is an isomorphism of R-algebras. Let us denote the elements $e := \Phi^{-1}(1_U, 0_V) \in A$ and likewise $f := \Phi^{-1}(0_U, 1_V)$. Then it is clear that $e^2 = \Phi^{-1}(1_U^2, 0_V) = \Phi^{-1}(1_U, 0_V) = e$ and for any $x = \Phi^{-1}(u, v)$ we get

$$\begin{aligned} xe &= \Phi^{-1}(u,v)\Phi^{-1}(1_U,0_V) = \Phi^{-1}(u,0_V) \\ &= \Phi^{-1}(1_U,0_V)\Phi^{-1}(u,v) = ex \end{aligned}$$

Hence we get $e \in \mathrm{CIP}(A)$ which by assumption is $e = 0$ or $e = 1$. In case $e = 0 = \Phi^{-1}(0_U, 0_V)$ we

have $1_P = 0_P$ such that $P = 0$ and in case $e = 1\Phi^{-1}(1_U, 1_V)$ we have $0_Q = 1_Q$ such that $Q = 0$. Altogether A is indecomposable, as claimed.

By now we have established the equivalence of (a) $\iff$ (c) $\iff$ (d) $\iff$ (e). Let us abbreviate $C := \mathrm{cen}(A) \leq_{\mathrm{a}} A$, then we will now prove (a) $\implies$ (b): if A is indecomposable, then by (e) we have $\mathrm{cip}(A) = \{0, 1\}$. In particular this means $\mathrm{cip}(C) = \{0, 1\}$ such that C satisfies (e) as well. And we already know that this implies (b). Conversely for (b) $\implies$ (a): if C is indecomposable, then by (d) $1 \in C$ is simple. That is there is no non-trivial decomposition $1 = e \oplus f$ with e, $f \in \mathrm{cen}(C) = C = \mathrm{cen}(A)$. Hence $1 \in A$ is simple as an element of A, as well. But this is (d) for A, such that A is indecomposable, itself.

□

Proof of (3.96):
Suppose X is a generating set of M with $|X| = \mathrm{rank}(M)$. As $\varphi : M \twoheadrightarrow N$ is surjective, for any $y \in N$ there is some $x \in M$ such that $y = \varphi(x)$. Also as X generates M we can choose some $a_i \in R$ and $x_i \in X$ such that $x = a_1x_1 + \cdots + a_nx_n$. And clearly this yields

$$y \;=\; \varphi(x) \;=\; \sum_{i=1}^{n} a_i\varphi(x_i) \;\in\; \mathrm{Lh}\Big(\varphi(X)\Big)$$

As $y \in N$ has been chosen arbitarily we have just seen, that $N = \mathrm{Lh}(\varphi(X))$. And from this we find the first inequality

$$\mathrm{rank}(N) \;\leq\; |\varphi(X)| \;\leq\; |X| \;=\; \mathrm{rank}(M)$$

For the second inequality choose some generating sets $X \subseteq P$ of P and $V \subseteq M/P$ of M/P such that $\mathrm{rank}(P) = |X|$ and $\mathrm{rank}(M/P) = |V|$. By construction of M/P any $v \in V$ is of the form $u + P$ for some $u \in M$. Thus for any $v \in V$ we may pick up some $u \in M$ such that $v = u + P$. We now take those u to build up a set $U \subseteq M$, that is we have $V = \{\, u + P \mid u \in U \,\}$ and $|U| = |V|$. We will now show, that $X \cup U$ generates M. To do this consider any $x \in M$: as $x + P \in M/P = \mathrm{Lh}(V)$ there are some $a_i \in R$ and $u_i \in U$ such that

$$x + P \;=\; \sum_{i=1}^{m} a_i(u_i + P) \;=\; \left(\sum_{i=1}^{n} a_iu_i\right) + P$$

That is $x - (a_1u_1 + \cdots + a_mu_m) \in P$. From this again we find some $b_j \in R$ and $p_j \in X$ such that $x - (a_1u_1 + \cdots + a_mu_m) = b_1p_1 + \cdots + b_np_n$ since X generates P. Altogether this yields

$$x \;=\; \sum_{i=1}^{m} a_iu_i + \sum_{j=1}^{n} b_jp_j \;\in\; \mathrm{Lh}(U \cup X)$$

Again, as $x \in M$ has been chosen arbitarily, this proves $M = \mathrm{Lh}(X \cup U)$, that is $X \cup U$ generates M and from this we get

$$\mathrm{rank}(M) \leq |P \cup U| \leq |P| + |U| = |P| + |V| = \mathrm{rank}(P) + \mathrm{rank}\left(M \Big/ P\right)$$

□

Proof of (3.99):

(i) If $n = 0$ then $X := \{ x_1, \ldots, x_n \}$ degenerates to $X = \emptyset$ and as X generates M this implies $M = 0$. Thus the only choice of an element $y_1 \in M$ is $y_1 = 0$ and this obviously is R-linear dependent. Thus we may assume $1 \leq n$. As M is the R-linear hull of X, we can choose some $a_{i,j} \in R$ (where $i \in 1 \ldots n$ and $j \in 1 \ldots n+1$) such that

$$y_j \;=\; \sum_{i=1}^{n} a_{i,j}\, x_i$$

Using these elements we first define the $\mathbb{Z}$-subalgebra S of R generated by the $a_{i,j}$. That is, we let

$$S \;:=\; \mathbb{Z}\left[a_{i,j} \mid i \in 1 \ldots n,\, j \in 1 \ldots n+1\right]$$

Note that $\mathbb{Z}$ is a noetherian ring (even a PID, by (2.71)) and S is a finitely generated $\mathbb{Z}$-algebra (by construction). Hence by the Hilbert basis theorem (2.42) S is a noetherian ring again. We now take to the S-module generated by the x_i

$$M_S \;:=\; \mathsf{Lh}_S \{ x_1, \ldots, x_n \}$$

Now, as M_S is a finitely generated S-module and S is a noetherian ring, M_S is a noetherian S-module, according to (3.111.(vi)). And clearly

$$y_j \;=\; \sum_{i=1}^{n} a_{i,j}\, x_i \;\in\; M_S$$

We will now recursively define the elements $y_j[m] \in M_S$ for any index $j \in 1 \ldots n+1$ and any $m \in \mathbb{N}$. We start by taking $y_j[0] := y_j$, then we continue

$$y_j[m+1] \;:=\; \sum_{i=1}^{n} a_{i,j}\, y_i[m]$$

To streamline our notation let us abbreviate $z_m := y_{n+1}[m]$. Now suppose that $Y := \{ y_1, \ldots, y_n, y_{n+1} \}$ was R-linearly independent. As $S \leq_{\mathsf{r}} R$ is a sub-ring of R, then in particular Y would be S-linearly independent. In an intermediate claim we will prove, that in this case the elements

$$y_1[m],\, \ldots,\, y_n[m],\, z_m = y_{n+1}[m],\, z_0,\, \ldots,\, z_{m-1}$$

are S-linearly independent for any $m \in \mathbb{N}$. The case $m = 0$ is trivial, as $y_j[0] = y_j$ our assumption on the y_j grants their S-linear independence. Let us use induction on m, then for the induction step we have to regard an S-linear relation of the form

$$\sum_{j=1}^{n+1} a_j\, y_j[m+1] + \sum_{l=0}^{m} b_l\, z_l \;=\; 0$$

Let us insert the recursive definition for the $y_j^{(m+1)}$ into this relation, then we find a relation of the

form

$$\begin{aligned} 0 &= \sum_{j=1}^{n+1} a_j y_j[m+] + \sum_{l=0}^{m} b_l z_l \\ &= \sum_{j=1}^{n+1} a_j \sum_{i=1}^{n} a_{i,j} y_i[m] + \sum_{l=0}^{m} b_l z_l \\ &= \sum_{i=1}^{n} \left(\sum_{j=1}^{n+1} a_j a_{i,j} \right) y_i[m] + \sum_{l=0}^{m-1} b_l z_l + b_m y_{n+1}[m] \end{aligned}$$

By the induction hypothesis these elements are S-linearly independent, such that we find $b_l = 0$ for any $l \in 1 \dots m$ and for any $i \in 1 \dots n$ also

$$\sum_{j=1}^{n+1} a_j a_{i,j} = 0$$

But this allows to give a linear relation between the y_j, just use the definition of the $a_{i,j}$ and compute (in the same manner as before)

$$\sum_{j=1}^{n+1} a_j y_j = \sum_{i=1}^{n} \left(\sum_{j=1}^{n+1} a_j a_{i,j} \right) x_i = 0$$

But by assumption the y_j are S-linearly independent, such that we necessarily have $a_j = 0$ for any $j \in 1 \dots n+1$ as well. Altogether we have proved the intermediate claim of linear independance. In particular the elements z_0, z_1, z_2 and so on are S-linearly independent. Thus - if we define

$$M_m := \mathrm{Lh}_S \{ z_l \mid l \in 0 \dots m \}$$

We get an ascending chain $M_0 \subseteq M_1 \subseteq M_2 \subseteq \dots$ of S-sub-modules of M_S. Yet this chain is strictly increasing: suppose we had $z_{m+1} \in M_m$ for some $m \in \mathbb{N}$ then there would be some $s_0, \dots, s_m \in S$ such that

$$z_{m+1} = \sum_{l=0}^{m} s_l z_l$$

which contradicts the S-linear independence of the z_l and hence we have $M_0 \subset M_1 \subset M_2 \subset \dots$. But a strictly increasing chain within the *noetherian* module M_S is impossible. The only way to solve this contradiction is to drop the assumption of R-linear independence of the y_j. That is Y is R-linear dependent, as we had claimed.

(ii) As $\{ m_1, \dots, m_n \}$ is a basis of M we obtain a well-defined endomorphism of R-modules, by letting

$$\varphi : M \to M : \sum_{i=1}^{n} a_i m_i \mapsto \sum_{i=1}^{n} a_i x_i$$

As $\{ x_1, \dots, x_n \}$ generates M this endomorphism is surjective. But then we can apply (3.82.(i)) to find that φ also is injective. That is if $\sum_i a_i x_i = 0$ then $\sum_i a_i m_i = 0$. But as the m_i are linearly independent this means $a_i = 0$ for any $i \in 1 \dots n$. And this is the linear independence of the x_i again.

(iii) Since the basis B by definition generates M as an R-module and the rank of M is the *minimal* cardinality of a generating set, trivially

$$\mathrm{rank}(M) \;\leq\; |B|$$

It remains to prove the equality. Let us choose some generating set $G \subseteq M$ of minimal cardinality, that is $|G| = \mathrm{rank}(M)$.

In a first step we assume that $n := |G| \in \mathbb{N}$ is finite. Suppose we had $n < |B|$, then we could choose some $\{ b_1, \ldots, b_n, b_{n+1} \} \subseteq B$. But as G generates M this would mean, that $\{ b_1, \ldots, b_n, b_{n+1} \}$ is R-linearly dependent, according to (i). But this contradicts the R-linear independence of B and hence we have

$$\mathrm{rank}(M) \;=\; |G| \;=\; n \;=\; |B|$$

In the second step, we suppose that $|G|$ is infinite. Then necessarily B is infinite as well - else we would have $|B| < |G| = \mathrm{rank}(M)$. As G generates M, for any $b \in B \subseteq M$, we can choose a *finite* subset $F_b \subseteq G$ such that $b \in \langle F_b \rangle_{\mathfrak{m}}$. Now define

$$F \;:=\; \bigcup_{b \in B} F_b \;\subseteq\; G$$

Then as B generates M and any $b \in B$ is generated by $F_b \subseteq F$ it is clear, that F also is a generating set of the entire module M:

$$\langle F \rangle_{\mathfrak{m}} \;=\; \sum_{b \in B} \langle F_b \rangle_{\mathfrak{m}} \;\supseteq\; \sum_{b \in B} Rb \;=\; \mathrm{Lh}_R(B) \;=\; M$$

Since any F_b has been finite, but B is infinite the cardinality of F is precisely the cardinality of B. But as $F \subseteq G$ this already yields the converse inequality

$$|B| \;=\; |F| \;\leq\; |G|$$

(iv) Choose some generating set $X \subseteq M$ of M with $|X| = \mathrm{rank}(M)$. Further, as F is free, we can choose some basis $B \subseteq F$ of F. Let us first suppose X is a finite set, say $X = \{ x_1, \ldots, x_n \}$. The basis $B \subseteq M$ is an R-linearly independent set, and hence B cannot contain more than n elements, as we have seen in (i). Hence by (ii) we have

$$\mathrm{rank}(F) \;=\; |B| \;\leq\; n \;=\; |X| \;=\; \mathrm{rank}(M)$$

So let us now consider the case that X is infinite - this will require some slight tricks of cardinal arithmetic: As X generates $M = \mathrm{Lh}(X)$ for any $y \in B$ there is a finite set $\omega(y) \subseteq X$ such that $y \in \mathrm{Lh}(\omega(y))$. Hence there is a map from B to the set $\Omega(X) := \{ Z \subseteq X \mid \#Z < \infty \}$ of finite subsets of X, given by

$$\omega \;:\; B \to \Omega(X) \;:\; y \mapsto \omega(y)$$

But as X is infinite we have $|X| = |\Omega(X)|$. Now consider any finite subset $Z \in \Omega(X)$, say $Z = \{ z_1, \ldots, z_n \} \subseteq X$. Then the fiber of Z is given to be $\omega^{-1}(Z) = \{ y \in B \mid \omega(y) = Z \}$. Thereby $\omega(y) = Z$ yields $y \in \mathrm{Lh}(\omega(y)) = \mathrm{Lh}(Z)$. Note that since $\omega^{-1}(Z) \subseteq B$ is contained in

the basis B of F it is R-linearly independent. And as $\mathrm{Lh}(Z)$ is generated by at most n elements (i) implies, that $\omega^{-1}(Z)$ cannot contain more that n elements: $\#\omega^{-1}(Z) \leq \#Z$. Thus any fiber of ω is finite. This now means, that the cardinality of B cannot exceed the cardinality of $\Omega(X)$. And altogether that is

$$\mathrm{rank}(F) \;=\; |B| \;\leq\; |\Omega(X)| \;=\; |X| \;=\; \mathrm{rank}(M)$$

□

Proof of (3.97):
If $\Phi : M \;\cong_{\mathsf{m}}\; N$ is an isomorphism of R-modules, then in particular $\Phi : M \twoheadrightarrow N$ is an epimorphism. Hence by (3.96) we find that $\mathrm{rank}(N) \leq \mathrm{rank}(M)$. But as the inverse $\Phi^{-1} : N \twoheadrightarrow M$ is surjective as well, we also have $\mathrm{rank}(M) \leq \mathrm{rank}(N)$. Altogether we have found

$$\mathrm{rank}(M) \;=\; \mathrm{rank}(N)$$

Conversely suppose that $\mathrm{rank}(M) = \mathrm{rank}(N)$. As both M and N are free we may choose bases $A \subseteq M$ of M and $B \subseteq N$ of N. As R is commutative and non-zero we may invoke (3.99.(iii)) to see

$$|A| \;=\; \mathrm{rank}(M) \;=\; \mathrm{rank}(N) \;=\; |B|$$

That is there is some bijection $\sigma : A \longleftrightarrow B \subseteq N$. As A is a basis of M we may now expand this map linearly. That is we use (3.72.(ii)) to define an R-module homomorphism

$$\Phi : M \to N : \sum_{x\in A} a_x x \mapsto \sum_{x\in A} a_x \sigma(x) \;=\; \sum_{y\in B} a_{\sigma^{-1}(y)} y$$

Likewise, as B is a basis as well, we can linearly expand $\sigma^{-1} : B \longleftrightarrow A \subseteq M$, as well. Then it is immediately clear, that $\Phi\Psi = \mathbb{1}_M$ and $\Psi\Phi = \mathbb{1}_N$. That is $\Phi : M \to N$ is an isomorphism with inverse $\Phi^{-1} = \Psi$. In particular we have $\Phi : M \;\cong_{\mathsf{m}}\; N$ as we had claimed. □

Proof of (3.102):

(i) Of course the proof will be an application of the lemma of Zorn. So let us regard the collection of all R-lineary independent subsets $L' \subseteq M$ containing L, formally that is

$$\mathcal{L} \;:=\; \left\{\, L' \subseteq M \mid L' \text{ is } R\text{-lineary independent}, L \subseteq L' \,\right\}$$

It is clear that $L \in \mathcal{L}$ and hence $\mathcal{L} \neq \emptyset$ is non-empty. Also $\mathcal{L}$ is partially ordered under the inclusion $\subseteq$. Now consider some chain $(L_i) \subseteq \mathcal{L}$ (where $i \in I$) in $\mathcal{L}$ and let

$$L' \;:=\; \bigcup_{i\in I} L_i \;\subseteq\; M$$

In order to establish $L' \in \mathcal{L}$ we have to show that L' is R-linearly independent again. Thus consider any $x_k \in L'$ and any $a_k \in R$ (where $k \in 1 \ldots n$) such that

$$a_1 x_1 + \cdots + a_n x_n \;=\; 0$$

By construction of L' for any $i \in 1 \ldots k$ there is some $i(k) \in I$ such that $x_k \in L_{i(k)}$. Since the L_i

form a chain we can assume (by renumbering the x_k), that

$$L_{i(1)} \subseteq L_{i(2)} \subseteq \ldots \subseteq L_{i(n)}$$

In particular $x_k \in L_{i(n)}$ for any $k \in 1 \ldots n$. But as $L_{i(n)}$ is linearly independent (it is contained in $\mathcal{L}$) the above equality implies $a_1 = \cdots = a_n = 0$. Hence L' is linearly independent, as well, such that $L' \in \mathcal{L}$. Hence every chain in $\mathcal{L}$ has an upper bound so that we may invoke the lemma of Zorn, to find a maximal element of $\mathcal{L}$.

(ii) If $x \in L$, then $x \in \mathrm{Lh}(L)$ is clear, such that we may take $a = 1$. Also if there is some $a \neq 0$ with $ax = 0$, then there is nothing to prove. So from now on we assume $x \notin L$ and $ax = 0 \implies a = 0$ for any $a \in R$. Then, as L is a maximal linear indepenedent set, $L \cup \{ x \}$ is no longer linear independent. That is there are some $y_1, \ldots, y_n \in L$ and some $a, b_1, \ldots, b_n \in R$ that are not identically zero, such that

$$ax + b_1 y_1 + \cdots + b_n y_n = 0$$

Thereby $ax = 0$ cannot be, as else $\{ y_1, \ldots, y_n \} \subseteq L$ would be linearly dependent. And by assumption this already implies $a \neq 0$. Now we see, that $ax = -(b_1 y_1 + \cdots + b_n y_n) \in \mathrm{Lh}(L)$ holds true as well.

(iii) By definition $\mathrm{free}(M) = 0$ means that $\emptyset \subseteq M$ is a maximal linearly independent set. This happens iff for any $x \in M$ the set $\{ x \} \subseteq M$ is linearly dependent already. The latter means that there is some $0 \neq a \in R$ such that $ax = 0$. And this again is precisely the property of M being a torsion module.

(iv) If L is a linearly independent set of M, then clearly $F := \mathrm{Lh}(L)$ is generated by L (by construction) and L is linearly independent (by assumption). That is L is a basis of F and F is free. If now $R \neq 0$ is a non-zero commutative ring, then lemma (3.99.(iv)) yields

$$|L| = \mathrm{rank}(F) \leq \mathrm{rank}(M)$$

(v) If $n = 0$ then $M = F$ and hence M is free with basis L itself. In particular L is a maximal linear independent subset of M and there is nothing to prove. Now suppose $n \geq 1$ the assumption that $L \cup \{ x_i \}$ is linearly dependent means that there are some $a_i \in R$ and $a_{i,u} \in R$ such that

$$a_i x_i + \sum_{u \in L} a_{i,u} u = 0$$

Note that this sum is finite only, since only finitely many $a_{i,u}$ are non-zero. Thereby $a_i \neq 0$ as else L would have been linearly dependent already. For later use define

$$a := \prod_{i=1}^{n} a_i \neq 0$$

Thereby $a \neq 0$ since all the $a_i \neq o$ and R is assumed to be an integral domain. Also note that $a/a_i \in R$ is a well-defined element of R. We will now prove that M/F is a torsion module: To see

this consider any $y \in M$ then, since $M = F + \mathrm{Lh}\{ x_1, \ldots, x_n \}$, we may write y in the form

$$y \;=\; f + \sum_{i=1}^{n} b_i x_i$$

for some $f \in F$ and $b_i \in R$. Then we will show $ay \in F$ using a staightforward computation

$$\begin{aligned} ay &= af + \sum_{i=1}^{n} a b_i x_i \\ &= af + \sum_{i=1}^{n} b_i \frac{a}{a_i} a_i x_i \\ &= af - \sum_{i=1}^{n} b_i \frac{a}{a_i} \sum_{u \in L} a_{i,u} u \\ &= af - \sum_{u \in L} \left(\sum_{i=1}^{n} b_i \frac{a}{a_i} a_{i,u} \right) u \end{aligned}$$

As the $u \in L$ generate F we see that truly $ay \in F$. But from this we find, that L is a maximal linearly independent set. Consider any $L' \subseteq M$ with $L \subseteq L'$. If there was some $y \in L' \setminus L$ then we have some $a \in R$ with $a \neq 0$ and $ay \in F = \mathrm{Lh}(L)$. Hence $L \cup \{ y \}$ and therefore L' are linearly dependent. And in particular we have the equalities

$$\mathrm{free}(M) \;=\; |L| \;=\; \dim(F)$$

If also follows that M/F is a torsion module: Consider any $y + F \in M/F$ then $a(y+F) = ay + F = 0 + F = 0 \in M/F$. And this is all that has been claimed.

(vi) We first prove that M/F where $F = \mathrm{Lh}(L)$ is a torsion module. Hence we consider any $z = x + F \in M/F$. As L is maximal linear independent (iii) yields some $a \in R$ with $a \neq 0$ such that $ax \in F$. Hence

$$az \;=\; ax + F \;=\; 0 + F \;=\; 0 \;\in\; M \Big/ F$$

And if $F \;\leq_{\mathrm{m}}\; M$ is a free sub-module of M with basis B, then $B \subseteq M$ clearly is linearly independent. It remains to prove the maximality of B. Thus suppose $B \subseteq X$. If there is some $x \in X$ with $x \notin B$, then (as M/F is a torsion module) we can choose some $a \in R$ with $a \neq 0$ such that $a(x + F) = 0 + F$. As above that is $ax \in F = \mathrm{Lh}(L)$. That is there are some $b_1, \ldots, b_n \in R$ and $y_1, \ldots, y_n \in B$ such that

$$ax \;=\; b_1 y_1 + \cdots + b_n y_n$$

Thus $b_1 y_1 + \cdots + b_n y_n - ax = 0$ is a linear relation with $a \neq 0$ within the set X. That is X is not linearly independent and hence $B \subseteq M$ is maximally linear independent.

(vii) We will first prove that $|L| = |L'|$. To do this we regard the map $\alpha : L \to L' : x \mapsto a_x x$. By definition of L' it is clear that α is surjective. Thus it remains to show the injectivity: suppose there were some $x, y \in L$ such that $x \neq y$ and $a_x x = a_y y$. Then

$$a_x x - a_y y \;=\; 0$$

As $\{ x, y \} \subseteq L$ is linear independent, this would imply $a_x = a_y = 0$ in contradiction to the choice of a_x and a_y. Hence α also is injective, that is we have established the bijecton $\alpha : L \longleftrightarrow L'$.

It remains to prove the linear independence of L'. Suppose we are given some $x(k) \in L'$ and $b(k) \in R$ (where $k \in 1 \dots n$) such that

$$0 \;=\; b(1)a(1)x(1) + \cdots + b(n)a(n)x(n)$$

Hereby we denoted $a(k) := a_{x(k)} \in R$. As $\{ x(1), \dots, x(n) \} \subseteq L$ is linear independent this implies $b(k)a(k) = 0$ for any $k \in 1 \dots n$. But as R is an integral domain and $a(k) \neq 0$ this already is $b(k) = 0$ for any $k \in 1 \dots n$. That is L' also is linearly independent.

(viii) As L is a maximal linear independent set, we have seen in (ii) that for any $x \in K$ there is some $a_x \in R$ with $a_x \neq 0$ and $a_x x \in Q := \mathrm{Lh}(L)$. Let us now denote $K' := \{ a_x x \mid x \in K \}$ and $P := \mathrm{Lh}(K')$. By (iv) we know, that K' is linearly independent again and hence P is a free submodule of M with basis K'. In fact, as $K' \subseteq Q$ we even have $P \subseteq Q$. Now by (3.99.(iii)) again we find

$$|K| \;=\; |K'| \;=\; \mathrm{rank}(P) \;\leq\; \mathrm{rank}(Q) \;=\; |L|$$

Reversing the roles of K and L in the above argument we also see that $|L| \leq |K|$ and hence $|K| = |L|$.

(ix) According to (i) we may pick up maximal linear independent sets $K \subseteq P$ and $\{ y + P \mid y \in L \} \subseteq M/P$ for some sufficient $L \subseteq M$. First of all it is clear, that $K \cap L = \emptyset$, because if we had $x \in K \cap L$ then $x \in K \subseteq P$ and hence $x + P = 0 + P$ such that $\{ x + P \}$ would be linearly dependent in contrast to $x \in L$. Hence we have $|K \cup L| = |K| + |L|$. It remains to prove that $K \cup L$ is a maximal linear independent set in M, as we then have

$$\mathrm{free}(M) \;=\; |K \cup L| \;=\; |K| + |L| \;=\; \mathrm{free}(P) + \mathrm{free}\left(M \Big/ P \right)$$

For the linear independence of $K \cup L$ suppose we have some $x_i \in K$ (where $i \in 1 \dots m$) and $y_j \in L$ (where $j \in 1 \dots n$) such that

$$z \;:=\; a_1 x_1 + \cdots + a_m x_m + b_1 y_1 + \cdots + b_n y_n \;=\; 0$$

for some a_i and $b_j \in R$. As $x_i \in K \subseteq P$ we then find that $0 + P = z + P = \sum_j b_j y_j + P = \sum_j b_j (y_j + P)$. But as $y_j \in L$ we know that the $y_j + P$ are linearly independent and hence necessarily $b_1 = \cdots = b_n = 0$. That is $0 = z = \sum_i a_i x_i$, but as the x_i are linearly independent as well, this implies $a_1 = \cdots = a_m = 0$ once more. Hence there only are trivial linear relations in $K \cup L$, that is $K \cup L$ is linearly independent.

It remains to prove the maximality of $K \cup L$. Hence suppose we are given any $z \in M$ with $z \notin K \cup L$. As $z + P \in M/P$ and $\{ y + P \mid y \in L \}$ is a maximal linear independent set (ii) implies that there is some $c \in R$ with $c \neq 0$ such that $cz + P \in \mathrm{Lh}(y + P \mid y \in L)$. That is there are some $y_j \in L$ and $b_j \in R$ (where $j \in 1 \dots n$ again) such that $cz + P = \sum_j b_j (y_j + P) = \sum_j b_j y_j + P$. That is $cz - \sum_j b_j y_j \in P$. And as $K \subseteq M$ is a maximal linear set as well (ii) once more implies that there

is some $d \in R$ with $d \neq 0$ such that $d(cz - \sum_j b_j y_j) \in \mathrm{Lh}(K)$. Altogether that is

$$d\left(cz - \sum_{j=1}^{n} b_j y_j\right) \;=\; \sum_{i=1}^{m} a_i x_i$$

for some $x_i \in K$ and $a_i \in R$ (where $i \in 1 \ldots m$ again). Rearranging this we found $dcz - (\sum_i a_i x_i + \sum_j db_j y_j) = 0$. Thereby $dc \neq 0$, as $c \neq 0$ and $d \neq 0$ and R is an integral domain. That is we have found a non-trivial linear relation in $K \cup L \cup \{ z \}$ which means that this set is linearly dependent. So at last $K \cup L$ is maximal linear independent.

(x) Let $L = \{ m_i \mid i \in I \} \subseteq M$ be a maximal linearly independent set in M and define $F := \mathrm{Lh}(L)$ again. Then F is a free R-module having the basis L. Now by (3.160.(i)) $\{ 1 \otimes m_i \mid i \in I \} \subseteq E \otimes M$ is an E-basis of $E \otimes M$ and hence

$$\dim_E(E \otimes M) \;=\; \dim_R(F) \;=\; |L| \;=\; \mathrm{free}(M)$$

□

Proof of (3.104):
The proof of theorem (i) is elementary, but not the easiest one. We have tried to increase its readability by presenting each step separately. It also makes use of the *well-ordering theorem* - a classical result from set-theory. there also is a direct proof of the theorem presented in [Adkins, Weintraub, 3.6.2]. However this proof is rather lengthy and intricate, such that we prefer this version:

(1) First of all, let $\{ m_i \mid i \in I \}$ be a basis of M. We now choose a well-ordering $\leq$ on I. Then for any $j \in I$ we denote the following sub-modules of M:

$$\begin{aligned} M_j &:= \mathrm{Lh}(m_i \mid i \leq j) \\ L_j &:= \mathrm{Lh}(m_i \mid i < j) \end{aligned}$$

It is clear that $i \leq j$ there by imples $M_i \subseteq M_j$ due to the transitivity of $\leq$. In fact we also get $M_j = L_j \oplus Rm_j$ but we do not require this fact. Instead let us denote further sub-modules of P:

$$\begin{aligned} P_j &:= M_j \cap P \\ K_j &:= L_j \cap P \end{aligned}$$

Again it is clear that $i \leq j$ now implies $P_i \subseteq P_j$ as this inherited from the M_j. But in this case we only have $K_j \subseteq P_j \subseteq P$ and it may well be, that $K_j = P_j$. In the following we will analyze the difference (i.e. quotient) between L_j and K_j. To do this we finally need to denote the coefficient map

$$\pi_j \;:\; M \to R \;:\; \sum_{i \in I} a_i m_i \;\mapsto\; a_j$$

The restriction of π_j to P_j will be denoted by φ_j. That is φ_j is to be the following R-module-homomorphism

$$\pi_j \;:\; P_j \to R \;:\; \sum_{i \in I} a_i m_i \;\mapsto\; a_j$$

(2) Clearly the kernel of π_j is the linear hull of $\{ m_i \mid i \neq j \}$. And if this is intersected with M_j there only remains L_j. In consequence the kernel of φ_j is nothing but K_j:

$$\mathrm{kn}(\varphi_j) \;=\; \mathrm{kn}(\pi_j) \cap P_j \;=\; \mathrm{kn}(\pi_j) \cap M_j \cap P \;=\; L_j \cap P \;=\; K_j$$

And as $im(\varphi_j) \;\leq_{\mathrm{m}}\; R$ is an R-sub-module, it even is an ideal in R (since R is commutative). But as R even is a PID, there has to be some $a_j \in R$ such that $im(\varphi_j) = a_j R$. In particular (if $a_j \neq 0$) we have the following isomorphy of R-modules

$$R \;\xrightarrow{\sim}\; \mathrm{im}(\varphi_j) \;:\; \lambda \mapsto a_j \lambda$$

(it is injective, since R is an integral domain and surjective by construction). But as $\mathrm{kn}(\varphi_j) = K_j$ and $im(\varphi_j) = a_j R$ the first isomorphism theorem (3.78.(ii)) have the following isomorphy of

$$P_j \Big/ K_j \;\xrightarrow{\sim}\; a_j R \;\;:\;\; x + K_j \mapsto \pi_j(x)$$

Note that clearly $K_j = L_j$ is equivalent to $a_j = 0$. Also note that in case $a_j \neq 0$ the inverse of the isomorphism $\lambda \mapsto a_j \lambda$ is given by $b \mapsto b/a_j$. Thus combining these two isomorphies we find the following isomorphy of R-modules

$$\Phi_j \;:\; P_j \Big/ K_j \;\xrightarrow{\sim}\; R \;:\; x + K_j \mapsto \frac{\pi_j(x)}{a_j}$$

That is to say that for any $x \in P_j$ we have established the equality $\pi_j(x) = a_j \Phi_j(x + k_j)$. Or more intuively speaking Φ_j yields the j-th coefficient of x once we scratch the a_j.

(3) For any $j \in J$ with $a_j \neq 0$ let us now choose some $p_j \in P_j$ such that $\Phi_j(p_j + K_j) = 1$. That is $\pi_j(p_j) = a_j$ - or intuitively speaking again: p_j is an element of P_j that hast a_j as its j-th coefficient. For formalities sake let us denote:

$$H \;:=\; \{ i \in I \mid a_i \neq 0 \}$$

We now claim that $\{ p_i \mid i \in H \}$ is an R-linearly independent set. That is we have to consider finitely many incides $i(1), i(2), \ldots, i(n) \in H$ with

$$\sum_{k=1}^{n} \lambda_{i(k)} p_{i(k)} \;=\; 0$$

for some coefficients $\lambda_{i(k)} \in R$. Scratching all the zero coefficients we may assume $\lambda_{i(k)} \neq 0$ for any $k \in 1 \ldots n$. By renumbering we may also assume $i(1) < i(2) < \cdots < i(n)$, as $\leq$ is a total order. But in consequence this yields the ascending chain of sub-modules of P, namely $P_{i(1)} \subseteq P_{i(2)} \subseteq \ldots \subseteq P_{i(n)}$. That is if $j := i(n)$ is the maximal index then we have $p_{i(k)} \in P_{i(k)} \subseteq P_j$ for any $k \in 1 \ldots n$. But then we get

$$0 \;=\; \varphi_j(0) \;=\; \sum_{k=1}^{n} \lambda_{i(k)} \varphi_j(p_{i(k)}) \;=\; \sum_{k=1}^{n} \lambda_{i(k)} a_j \delta_{i(k),j} \;=\; \lambda_j a_j$$

as $\varphi_j(p_{i(k)}) = \pi_j(p_{i(k)}) = a_j\delta_{i(k),j}$. But since $a_j \neq 0$ and R is an integral domain this means $\lambda_j = 0$ - a contradiction. Hence we must have scratched all coefficients $\lambda_{i(k)}$ which means there is no such sum. Altogether the linear independence of $\{\, p_i \mid i \in H \,\}$ is established.

(4) It remains to prove that $\{\, p_i \mid i \in H \,\}$ also generates P as an R-module (then it is a basis of P and we have $\mathrm{rank}(P) = |H| \leq |I| = \mathrm{rank}(M)$). To do this let us abbreviate

$$P_0 \;:=\; \mathrm{Lh}_R\{\, p_i \mid i \in H \,\} \;\subseteq\; P$$

As $\{\, m_i \mid i \in I \,\}$ is an R-basis of M for any $x \in M$ there are uniquely determined coefficients $\lambda_i \in R$ such that

$$x \;=\; \sum_{i\in I} \lambda_i m_i$$

Thereby the set $\{\, i \in I \mid \lambda_i \neq 0 \,\}$ has been finite. And as $\leq$ is a total order this enables us to introduce the maximal index $\mu(x)$ enumerating a non-zero coefficient of x, that is:

$$\mu(x) \;:=\; \max\{\, i \in I \mid \lambda_i \neq 0 \,\} \;\in\; I$$

We have to show $P_0 = P$ of course, so assume we had the contrary $P \setminus P_0 \neq \emptyset$. Then - as I even is well-ordered - there would be a minimal among these maximal indexes

$$\alpha \;:=\; \min\{\, \mu(x) \mid x \in P \setminus P_0 \,\} \;\in\; I$$

Recall that being minimal means that for any $x \in P \setminus P_0$ we have that $\mu(x) \leq \alpha$ implies $\mu(x) = \alpha$. Now consider any $x \in K_\alpha = L_\alpha \cap P$. Since $x \in L_\alpha$ we have $\mu(x) < \alpha$. And due to the minimality of α this implies $x \notin P \setminus P_0$. But as also $x \in P$ this only leaves $x \in P_0$ such that we have argued, that

$$K_\alpha \;\subseteq\; P_0$$

Now let us further pick up some element $u \in P \setminus P_0$ such that $\mu(u) = \alpha$ and let us denote its basis decomposition by

$$u \;=\; \sum_{k=1}^{n} \nu_{i(k)} m_{i(k)}$$

for some $\nu_{i(k)} \in R$ with $\nu_{i(k)} \neq 0$. Renumbering we may again assume, that $i(1) < i(2) < \cdots < i(n) = \alpha$. As $u \in M_\alpha$ and also $u \in P$ we have $u \in M_\alpha \cap P = P_\alpha$. And therefore we may regard $\nu_\alpha = \varphi_\alpha(u) \in a_\alpha R$. That is there is some $b \in R$ such that $\nu_\alpha = a_\alpha b$. By construction of the isomorphism Φ_α this means

$$\Phi_\alpha(u + K_\alpha) \;=\; b$$

As $\nu_\alpha \neq 0$ we also find $a_\alpha \neq 0$ and hence $bp_\alpha \in P_0$ by definition of P_0. Then we may compute

$$\Phi_\alpha(u - bp_\alpha + K_\alpha) = \Phi_\alpha(u + K_\alpha) - b\Phi_\alpha(p_\alpha + K_\alpha) = b - b \cdot 1 = 0$$

This means $u - bp_\alpha + K_\alpha = 0 + K_\alpha$ or in other words $u - bp_\alpha \in K_\alpha \subseteq P_0$. This again means $u + P_0 = bp_\alpha + P_0 = 0 + P_0$ such that $u \in P_0$ - a contradiction. Hence $P \setminus P_0$ must have been empty which is $P_0 = P$. That is $\{\, p_i \mid i \in H \,\}$ truly generates P as an R-module and hence is a

basis of P.

The proof of theorem (ii) is rather short in comparison: Let $\{ m_i \mid i \in I \}$ be a generating set of M where $|I| = \mathrm{rank}(M)$. We have the epimorphism

$$\mu \ : \ R^{\oplus I} \ \twoheadrightarrow \ M \ : \ (a_i) \mapsto \sum_{i \in I} a_i m_i$$

Let $P_0 := \mu^{-1}(P) \ \leq_{\mathsf{m}} \ R^{\oplus I}$. As $R^{\oplus I}$ is a free module [it has the Euclidean basis] over the PID R we know by (i) that P_0 is free as well and more importantly: $\dim(P_0) \leq \dim(R^{\oplus I}) = |I| = \mathrm{rank}(M)$. But as μ is surjective, we also have $\mu(P_0) = \mu\big(\mu^{-1}(P)\big) = P$ such that the restriction of μ to P_0 is an epimorphism onto P:

$$\mu \ : \ P_0 \ \twoheadrightarrow \ P \ : \ (a_i) \mapsto \sum_{i \in I} a_i m_i$$

In particular by (3.96) we have $\mathrm{rank}(P) \leq \mathrm{rank}(P_0) = \dim(P_0) \leq \mathrm{rank}(M)$. And if M is is finitely generated, then P is finitely generated as well, since $\mathrm{rank}(P) \leq \mathrm{rank}(M) < \infty$.
Next we prove (iii): If M is free, then it already is torsion-free, according to (3.23.(ii)), since R is an integral domain (even a PID). Conversely if M is torsion-free, then by (3.23.(iv)) - as M also is finitely generated - it is embedded $M \ \xrightarrow{\sim} \ N \ \leq_{\mathsf{m}} \ R^n$ into the free R-module R^n. But by (i) the sub-module N is free again, such that M has to be free, as well, due to the isomorphy to N.
Finally it remains to prove (iv): Generally - for any module, over any ring - we have the following short exact sequence of R-modules

$$0 \to \mathrm{TOR}(M) \ \xrightarrow{\subseteq} \ M \ \xrightarrow{\varrho} \ M \Big/ \mathrm{TOR}(M) \to 0$$

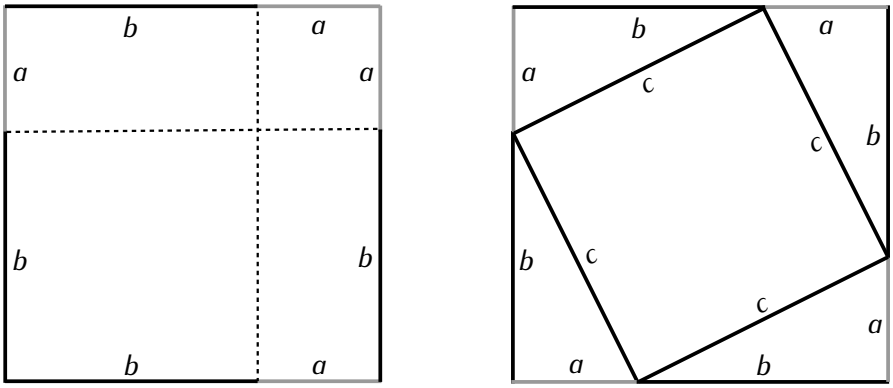
Since M is finitely generated so is $Q := M/\mathrm{TOR}(M)$. But as Q also is torsion-free, according to (3.23.(i)), (iii) tells us, that Q is free. But then (3.90) yields the desired isomorphy

$$M \quad \cong_{\mathsf{m}} \quad M \Big/ \mathrm{TOR}(M) \oplus \mathrm{TOR}(M)$$

□

15.5 Proofs of Chapter 4

Proof of (4.112):
Let us look at a square, whose length of its sides is $a+b$ in two separate ways: First we can decompose that square into a square of size a, a square of size b and two rectangles of size ab. On the other hand we can decompose said square into a square of size c and 4 triangles that fit the description of the lemma:



As it is the same square its area is equal, namely $(a+b)^2$. Every two triangles in the figure on the right side can be combined to a rectangle of area ab. Thus their area is $ab/2$. The decomposition of the square of size $a+b$ now yield two separate formulas for the area of the square

$$\begin{aligned}(a+b)^2 &= a^2+b^2+2\cdot ab\\ (a+b)^2 &= c^2+4\cdot\frac{ab}{2} \;=\; c^2+2\cdot ab\end{aligned}$$

Note that the first equality is just the binomial formula for $(a+b)^2$. As these two are equal we may subtract $2ab$ from the terms to find the desired pythagorean equality $c^2=(a+b)^2-2ab=a^2+b^2$. □

Proof of (4.8):

(i) It is clear that $\mathrm{mat}_{m,n}(R)$ is an R-module, as a matrix in nothing but a peculiar way of arranging an mn-tuple $A\in R^{mn}$. If this doesn't convince you try the following reasoning: $M:=R^m$ is a R-module under the point-wise operations. Hence $\mathrm{mat}_{m,n}(R)=M^n$ is an R-module under the point-wise operations, too. But the point-wise operations are precisely what we have taken for the addition and scalar-multiplication of matrices. And the fact that $\mathcal{E}$ is an R-basis follows immediately from (3.61.(vi)) once we notice, that any matrix $A=(a_{i,j})$ can be written uniquely, as

$$A \;=\; \sum_{i=1}^{m}\sum_{j=1}^{n} a_{i,j}\,E_{i,j}$$

(ii) We will first prove the associativity of the matrix multiplication. To do this fix any index $i\in 1\ldots m$ and $l\in 1\ldots q$ and compute

$$\mathrm{ent}_{i,l}((AB)C) \;=\; \sum_{k=1}^{p}\mathrm{ent}_{i,k}(AB)\,\mathrm{ent}_{k,l}(C)$$

$$\begin{aligned} &= \sum_{k=1}^{p}\sum_{j=1}^{n} \mathsf{ent}_{i,j}(A)\,\mathsf{ent}_{j,k}(B)\,\mathsf{ent}_{k,l}(C) \\ &= \sum_{j=1}^{n} \mathsf{ent}_{i,j}(A) \sum_{k=1}^{p} \mathsf{ent}_{j,k}(B)\,\mathsf{ent}_{k,l}(C) \\ &= \sum_{j=1}^{n} \mathsf{ent}_{i,j}(A)\,\mathsf{ent}_{j,l}(BC) \\ &= \mathsf{ent}_{i,l}(A(BC)) \end{aligned}$$

The distributivity can be proved by a direct computation as well. In this case we prefer to e4mploy the scalar product however:

$$\begin{aligned} \mathsf{ent}_{i,k}(A(B+C)) &= \langle \mathsf{row}_i(A), \mathsf{col}_k(B+C)\rangle \\ &= \langle \mathsf{row}_i(A), \mathsf{col}_k(B) + \mathsf{col}_k(C)\rangle \\ &= \langle \mathsf{row}_i(A), \mathsf{col}_k(B)\rangle + \langle \mathsf{row}_i(A), \mathsf{col}_k(C)\rangle \\ &= \mathsf{ent}_{i,k}(AB) + \mathsf{ent}_{i,k}(AC) \\ &= \mathsf{ent}_{i,k}(AB + AC) \\ \mathsf{ent}_{i,k}((A+B)C)) &= \langle \mathsf{row}_i(A+B), \mathsf{col}_k(C)\rangle \\ &= \langle \mathsf{row}_i(A) + \mathsf{row}_i(B), \mathsf{col}_k(C)\rangle \\ &= \langle \mathsf{row}_i(A), \mathsf{col}_k(C)\rangle + \langle \mathsf{row}_i(B), \mathsf{col}_k(C)\rangle \\ &= \mathsf{ent}_{i,k}(AC) + \mathsf{ent}_{i,k}(BC) \\ &= \mathsf{ent}_{i,k}(AC + AC) \end{aligned}$$

(iii) As mat_n is an R-module by (i) and the multiplication is associative and distributive by (ii) we already know that $\mathsf{mat}_n(R)$ is an R-semi-algebra. It remains to prove that $\mathbb{1}$ truly is a unit element in $\mathsf{mat}_n(R)$. To see this consider any $A \in \mathsf{mat}_n(R)$ and compute

$$\begin{aligned} \mathsf{ent}_{i,k}(\mathbb{1}\,A) &= \sum_{j=1}^{n} \mathsf{ent}_{i,j}(\mathbb{1})\,\mathsf{ent}_{j,k}(A) \\ &= \sum_{j=1}^{n} \delta_{i,j}\,\mathsf{ent}_{j,k}(A) \;=\; \mathsf{ent}_{i,k}(A) \\ \mathsf{ent}_{i,k}(A\,\mathbb{1}) &= \sum_{j=1}^{n} \mathsf{ent}_{i,j}(A)\,\mathsf{ent}_{j,k}(\mathbb{1}) \\ &= \sum_{j=1}^{n} \mathsf{ent}_{i,j}(A)\,\delta_{j,k} \;=\; \mathsf{ent}_{i,k}(A) \end{aligned}$$

(iv) The inverse generally is uniquely determined in associative grupoids, let us repeat the proof here: Suppose both B and $B' \in \mathsf{mat}_n(R)$ satisfy $AB = \mathbb{1}_n = BA$ and $AB' = \mathbb{1}_n = B'A$ respectively. Then we find $B = B'$ by a easy computation

$$B \;=\; B\mathbb{1}_n \;=\; B(AB') \;=\; (BA)B' \;=\; \mathbb{1}_n B' \;=\; B'$$

(v) We will first prove $\mathrm{cen}(R)\mathbb{1} \subseteq \mathrm{cen}(\mathrm{mat}_n(R))$, that is we consider any $a \in \mathrm{cen}(R)$ and $B = (b_{i,j}) \in \mathrm{mat}_n(R)$. Then we have to check that $(a\mathbb{1})B = B(a\mathbb{1})$. But as a commutes with all other elements of R this is quite easy to see:

$$(a\mathbb{1})B \;=\; a(\mathbb{1}B) \;=\; aB \;=\; (ab_{i,j}) \;=\; (b_{i,j}a) \;=\; B(a\mathbb{1})$$

Conversely consider any $A = (a_{i,j}) \in \mathrm{cen}(\mathrm{mat}_n(R))$, that is A is a matrix, that commutes with all other matrices. In particular we have $AE_{r,s} = E_{r,s}A$ for any $r, s \in 1 \ldots n$. Now evaluate the (i,k)th entry

$$\begin{aligned}
\mathrm{ent}_{i,k}(A\,E_{r,s}) &= \sum_{j=1}^{n} a_{i,j}\,\delta_{j,r}\,\delta_{k,s} \;=\; a_{i,r}\,\delta_{k,s} \\
\mathrm{ent}_{i,k}(E_{r,s}\,A) &= \sum_{j=1}^{n} \delta_{i,r}\,\delta_{j,s}\,a_{j,k} \;=\; \delta_{i,r}\,a_{s,k}
\end{aligned}$$

That is for any i, k, r and $s \in 1 \ldots n$ we have $a_{i,r}\delta_{k,s} = \delta_{i,r}a_{s,k}$. Let us choose $s := k$ then this equality specializes to

$$a_{i,r} \;=\; \delta_{i,r}\,a_{k,k}$$

In particular - by taking $r := i$ - we find $a_{i,i} = a_{k,k}$ for any indexes i, k. And if $r \neq i$, then we have $a_{i,r} = 0$. That is A is a diagonal matrix, in which all diagonal elements are equal. In short: A is of the form $A = a\mathbb{1}$ for some $a \in R$. Now take $B := b\mathbb{1}$, then clearly $AB = ab\mathbb{1}$ and $BA = ba\mathbb{1}$. But as $AB = BA$ and $b \in R$ is arbitrary, this implies $a \in \mathrm{cen}(R)$. Hence we also have $\mathrm{cen}(\mathrm{mat}_n(R)) \subseteq \mathrm{cen}(R)\mathbb{1}$.

(vi) Let $A = (a_{i,j})$ and $B = (b_{i,j})$ where $i, j \in 1 \ldots n$. Then by definition of the matrix-multiplication we have

$$\mathrm{ent}_{i,i}(AB) \;=\; \sum_{j=1}^{n} a_{i,j}b_{j,i}$$

Thus we find the equality of $\mathrm{tr}(AB)$ and $\mathrm{tr}(BA)$ using the following computation in which we rename the indices i and j [in the third step], use the commutativity of R [in the fourth step] and swap the summation symbols [in the fith step]

$$\begin{aligned}
\mathrm{tr}(AB) &= \sum_{i=1}^{n} \mathrm{ent}_{i,i}(AB) \;=\; \sum_{i=1}^{n}\sum_{j=1}^{n} a_{i,j}b_{j,i} \\
&= \sum_{j=1}^{n}\sum_{i=1}^{n} a_{j,i}b_{i,j} \;=\; \sum_{j=1}^{n}\sum_{i=1}^{n} b_{i,j}a_{j,i} \\
&= \sum_{i=1}^{n}\sum_{j=1}^{n} b_{i,j}a_{j,i} \;=\; \sum_{i=1}^{n} \mathrm{ent}_{i,i}(BA) \\
&= \mathrm{tr}(BA)
\end{aligned}$$

(vii) Let us first check, that $\varphi_A : R^n \to R^m$ truly is R-linear. Again this is a straightforward computation using the definition of the matrix-vector multiplication. Pick up $x, y \in R^n$ and $a \in R$, then for any

$i \in 1 \ldots m$

$$\begin{aligned}
[A(x+y)]_i &= \sum_{j=1}^{n} a_{i,j} [x+y]_j = \sum_{j=1}^{n} a_{i,j}(x_j + y_j) \\
&= \sum_{j=1}^{n} a_{i,j} x_j + \sum_{j=1}^{n} a_{i,j} y_j = [Ax]_i + [Ay]_i \\
[A(ax)]_i &= \sum_{j=1}^{n} a_{i,j} [ax]_j = \sum_{j=1}^{n} a_{i,j} a x_j \\
&= a \sum_{j=1}^{n} a_{i,j} x_j = a\,[Ax]_i
\end{aligned}$$

The latter, since R is commutative. As this is true for any $i \in 1 \ldots n$ and the operations in R^m are point-wise again, we have $A(x+y) = Ax + Ay$ and $A(ax) = a\,Ax$. Therefore $\varphi_A : x \mapsto Ax$ truly is in $\mathrm{mhom}(R^n, R^n)$ such that $A \mapsto \varphi_A$ is well-defined. Next we have to check, that this map a homomorphism of R-modules, that is $\varphi_{A+B} = \varphi_A + \varphi_B$ and $\varphi_{aA} = a\varphi_A$. But this has already been dealt with, in (ii):

$$\begin{aligned}
\varphi_{A+B}(x) &= (A+B)x = Ax + Bx = \varphi_A(x) + \varphi_B(x) \\
\varphi_{aA}(x) &= (aA)x = a(Ax) = a\varphi_A(x)
\end{aligned}$$

It remains to check the bijectivity of $A \mapsto \varphi_A$. We will do this by presenting the inverse map: If $\varphi : R^n \to R^m$ is R-linear, then take

$$[\varphi] := (a_{i,j}) \quad \text{where} \quad a_{i,j} := \big[\varphi(e_j)\big]_i$$

where $e_1 = (1, 0, \ldots, 0)$ to $e_n = (0, \ldots, 0, 1)$ denote the Euclidean basis vectors of R^n. Thus if $A = [\varphi]$ we have to check that $\varphi_A = \varphi$ and $[\varphi_A] = A$. The latter is straightforward:

$$\mathrm{ent}_{i,j}([\varphi_A]) = \big[\varphi_A(e_j)\big]_i = \big[Ae_j\big]_i = \big[\mathrm{col}_j(A)\big]_i = \mathrm{ent}_{i,j}(A)$$

And since this is true for any $i \in 1 \ldots m$ and any $j \in 1 \ldots n$ we have $[\varphi_A] = A$. If now $A = [\varphi]$ then $a_{i,j} = [\varphi(e_j)]_i$ and hence $\mathrm{col}_j(A) = (a_{1,j}, \ldots, a_{m,j}) = \varphi(e_j) \in R^m$. Therefore

$$\varphi_A(e_j) = Ae_j = \mathrm{col}_j(A) = \varphi(e_j)$$

Thus we have $\varphi_A(e_j) = \varphi(e_j)$ for any $j \in 1 \ldots n$ and as these for a basis of R^n and both φ_A and φ are R-linear we have $\varphi_A(x) = \varphi(x)$ for any $x \in R^n$. That is $\varphi_A = \varphi$ such that $\varphi \mapsto [\varphi]$ truly is the inverse map of $A \mapsto \varphi_A$. In particular $A \mapsto \varphi_A$ is bijective and hence an isomorphism of R-modules.

(viii) It is clear, that the transposition $A \mapsto A^*$ is bijective - the inverse map is the transposition $\mathrm{mat}_{n,m}(R) \to \mathrm{mat}_{m,n}(R) : B \mapsto B^*$ again. And the R-linearity of the transposition is straightforward again

$$\mathrm{ent}_{j,i}((aA+B)^*) = \mathrm{ent}_{i,j}(aA+B) = a\,\mathrm{ent}_{i,j}(A) + \mathrm{ent}_{i,j}(B)$$

$$= \quad a\,\mathrm{ent}_{j,i}(A^*) + \mathrm{ent}_{j,i}(B^*) \;=\; \mathrm{ent}_{j,i}(aA^* + B^*)$$

(ix) Recall that R is assumed to be commutative here. Let us compare all the entries of the matrices $(AB)^*$ and B^*A^*, $i \in 1\ldots l$ and $k \in 1\ldots n$. Then by definition of the matrix-multiplication we find that all entries are equal, just compute

$$\begin{aligned}\mathrm{ent}_{k,i}(B^*A^*) &= \langle \mathrm{row}_k(B^*), \mathrm{col}_i(A^*)\rangle \;=\; \langle \mathrm{col}_k(B), \mathrm{row}_i(A)\rangle \\ &= \langle \mathrm{row}_i(A), \mathrm{col}_k(B)\rangle \;=\; \mathrm{ent}_{i,k}(AB) \\ &= \mathrm{ent}_{k,i}((AB)^*)\end{aligned}$$

(x) Let us first assume that A is invertible, then an easy computation yields $\mathbb{1}_n = \mathbb{1}_n^* = (AA^{-1})^* = (A^{-1})^*A^*$ where the latter equality is due to (vi). Likewise $\mathbb{1}_n = (A^{-1}A)^* = A^*(A^{-1})^*$. Hence we have seen that in this case A^* is invertible, too and that the inverse is given to be $(A^{-1})^*$. That is we have proved the equality

$$(A^*)^{-1} \;=\; \left(A^{-1}\right)^*$$

If conversely A^* is invertible, then we have just seen that $(A^*)^* = A$ is invertible. So this already establishes the equivalence of the invertibilities of A and A^*.

(xi) Let us denote $x = (x_1,\ldots,x_n) \in R^n$ and $y = (y_1,\ldots,y_m) \in R^m$, then it is straightforward to compute

$$\begin{aligned}\langle Ax, y\rangle &= \sum_{i=1}^{m} [Ax]_i\, y_i \;=\; \sum_{i=1}^{m}\sum_{j=1}^{n} \mathrm{ent}_{i,j}(A)\, x_j\, y_i \\ &= \sum_{j=1}^{n} x_j \sum_{i=1}^{m} \mathrm{ent}_{i,j}(A)\, y_i \;=\; \sum_{j=1}^{n} x_j \sum_{i=1}^{m} \mathrm{ent}_{j,i}(A^*)\, y_i \\ &= \sum_{j=1}^{n} x_j\, [A^*y]_j \;=\; \langle x, A^*y\rangle\end{aligned}$$

□

Proof of (4.10):
If $u \in 1\ldots l = l(1) + \cdots + l(r)$ is any row-number of A, then there are some $i \in 1\ldots r$ and $u' \in 1\ldots l(i)$ such that the u-th row of A runs across the u'-th rows of $A^{i,1}$ to $A^{i,s}$. That is we can pick up $i \in 1\ldots r$ and $u' \in 1\ldots l(i)$ such that $u = u' + l(1) + \cdots + l(i-1)$. Likewise for a column-number $v \in 1\ldots n = n(1) + \cdots + n(t)$ of B, there are some $k \in 1\ldots t$ and $v' \in 1\ldots n(j)$ such that the v-th column of B runs across the v'-th columns of $B^{1,j}$ to $B^{s,j}$. Again we pick up $k \in 1\ldots t$ and $v' \in 1\ldots n(n)$ such that $v = v' + n(1) + \cdots + n(k-1)$.

Then the (u,v)-th entry of AB is given to be $\langle \mathrm{row}_u(A), \mathrm{col}_v(B)\rangle$. But as the u-th row of A and the v-th row of are concatenations of the u'-th rows of the $A^{i,j}$ and of the v'-th columns of the $B^{j,k}$ respectively

we find that

$$\mathsf{ent}_{u,v}(AB) \;=\; \langle \mathsf{row}_u(A), \mathsf{col}_v(B)\rangle \;=\; \langle \begin{pmatrix} \mathsf{row}_{u'}(A^{i,1}) \\ \vdots \\ \mathsf{row}_{u'}(A^{i,s}) \end{pmatrix}, \begin{pmatrix} \mathsf{col}_{v'}(B^{1,k}) \\ \vdots \\ \mathsf{col}_{v'}(B^{s,k}) \end{pmatrix} \rangle$$

By assumption on the compatible block-structure of A and B these rows and columns are of compatible sizes, too and hence we may conclude

$$\mathsf{ent}_{u,v}(AB) \;=\; \sum_{j=1}^{s} \langle \mathsf{row}_{u'}(A^{i,j}), \mathsf{col}_{v'}(B^{j,k})\rangle \;=\; \sum_{j=1}^{s} \mathsf{ent}_{u',v'}(A^{i,j}B^{j,k}) \;=\; \mathsf{ent}_{u',v'}\left(\sum_{j=1}^{s} A^{i,j}B^{j,k}\right)$$

If we now chunk up AB into the resulting block structure [i.e. we have r rows of the sizes $l(1)$ to $l(r)$ and t columns of the sizes $n(1)$ to $n(t)$] then the (u',v')-index of the sub-matrices corresponds to the (u,v)-index of the whole matrix and hence the proof is complete. □

Proof of (4.20):
Let us denote $X = (x_1, x_2, \ldots x_m) \in \mathsf{mat}_{p,m}(R)$ and $Y := (y_1, y_2, \ldots, y_n) \in \mathsf{mat}_{p,n}(R)$. Then by definition of the matrix multiplication, the (i,k)-th entry of XA is given to be

$$[XA]_{i,k} \;=\; \sum_{j=1}^{m} x_{i,j}a_{j,k}$$

Thereby $x_{i,j} = [x_j]_i$ is just the i-th component of $x_j \in R^p$. And as R was assumed to be commuttive this enables us to rewrite

$$[XA]_{i,k} \;=\; \sum_{j=1}^{m} a_{j,k}\left[x_j\right]_i \;=\; \left[\sum_{j=1}^{m} a_{j,k}x_j\right]_i$$

But by assumption this is just $[y_k]_i$. Thus we find that the k-th column of XA is just y_k and this is precisely the claim of this proposition. □

Proof of (4.14):
The definiton of $\mathsf{gl}_n(R)$ is precisely that of the multiplicative group of $\mathsf{mat}_n(R)$, hence there is nothing to prove.

It is clear that the unit element $\mathbb{1}_n$ of $\mathsf{mat}_n(R)$ is contained in $\mathsf{tri}_n(R)$. Also if A and $B \in \mathsf{tri}_n(R)$ are any two upper triangular matrices, then for any $a \in R$ and any $i, j \in 1 \ldots n$ we have

$$\mathsf{ent}_{i,j}(aA + B) \;=\; a\,\mathsf{ent}_{i,j}(A) + \mathsf{ent}_{i,j}(B)$$

In particular if $j < i$ we see that $\mathsf{ent}_{i,j}(aA + B) = 0$, such that $aA + B$ is an upper triangular matrix again. By taking $a = 1$ we see that $A + B \in \mathsf{tri}_n(R)$ and by taking $a = -1$ and $B = 0$ we also have $-A \in \mathsf{tri}_n(A)$. That is we have proved, that $(\mathsf{tri}_n(R), +)$ is a subgroup of $(\mathsf{mat}_n(R), +)$ - in fact we have shown that $\mathsf{tri}_n(R)$ is an R-sub-module of $\mathsf{mat}_n(R)$.

It remains to prove that $\mathsf{tri}_n(R)$ is closed under multiplication of matrices as well. Hence consider any two upper triangular matrices $A = (a_{i,j})$ and $B = (b_{i,j}) \in \mathsf{tri}_n(R)$ again. Then for any $i, k \in 1 \ldots n$ we

have

$$\mathrm{ent}_{i,k}(AB) \;=\; \sum_{j=1}^{n} a_{i,j}\, b_{j,k}$$

But since $A \in \mathrm{tri}_n(R)$ we have $a_{i,j} = 0$ for any $j < i$. And as $B \in \mathrm{tri}_n(B)$ as well, we also have $b_{j,k} = 0$ of any $j > k$. Hence the only summands which might be non-zero are those from $j = k$ to $j = i$. That is the sum breaks down to

$$\mathrm{ent}_{i,k}(AB) \;=\; \sum_{j=k}^{i} a_{i,j}\, b_{j,k}$$

Hence if $i < k$ there are no non-zero elements left at all and the sum is 0. But this precisely means that $AB \in \mathrm{tri}_n(R)$ is an upper triangular matrix again, and this had to be shown.

In the next step, let us prove the recursion formula for solving the SLE $Tx = b$. As $t_{i,j} = 0$ for any $i > j$ it is clear, that $Tx = b$ breaks down to the following equations (for any $i \in 1 \ldots n$)

$$\sum_{j=i}^{n} t_{i,j} x_j \;=\; b_i$$

In particular for $i = n$ we have $t_{n,n} x_n = b_n$. If now $t_{n,n} \in R^*$ is invertible, then we get $x_n = t_{n,n}^{-1} b_n$. Now suppose we have already computed x_n, x_{n-1} and so on, up to x_{i+1}. Then the i-th equation yields

$$t_{i,i} x_i + \sum_{j=i+1}^{n} t_{i,j} x_j \;=\; b_i$$

Thus if $t_{i,i} \in R^*$ is invertible, as well, we find precisely the recursion formula for x_i given in the claim

$$x_i \;=\; t_{i,i}^{-1} \left(b_i - \sum_{j=i+1}^{n} t_{i,j} x_j \right)$$

In particular: If any $t_{i,i} \in R^*$ then T is invertible. Let us now prove, that T^{-1} is an upper triangular matrix again. By (4.11) the j-th column of T^{-1} is x_j where $Tx_j = e_j$. That is we have to prove, that $[x_j]_i = \mathrm{ent}_{i,j}(T^{-1}) = 0$ whenever $i > j$. We do this recursively starting with $j = n$ and working our way down to $j = 1$. For $j = n$ the condition $i > j$ is void, the last column is irrelevant. Now consider $j < n$ and start with $i = n$, then $[x_j]_n = t_{n,n}^{-1} [e_j]_n = 0$. Suppose we have already proved $[x_j]_i = 0$ for $i = n$ down to $i = k + 1$, where $k > j$. Then we use the recursion formula again, to find

$$[x_j]_k \;=\; t_{k,k}^{-1} \left([e_j]_k - \sum_{l=k+1}^{n} t_{k,l} [x_j]_l \right)$$

As both $[e_j]_k = 0$ and $[x_j]_l = 0$ for $l \geq k + 1$, by assumption, we find $[x_j]_k = 0$ too. This changes, at $k = j$, as here $[e_j]_j = 1$ such that $[x_j]_j = t_{j,j}^{-1}$. Therefore we have proved two things: (1) T^{-1} is an upper triangular matrix again and (2) if T is invertible, then any $t_{j,j} \in R$ is an invertible element, too. □

Proof of (4.15):

We need to show, that $\mathrm{tri}_n^1(R)$ is a subgroup of $\mathrm{gl}_n(R)$. As $\mathbb{1}_n \in \mathrm{tri}_n^1(R)$ is trivial, we commence by proving, that $\mathrm{tri}_n^1(R)$ is closed under the multiplication of matrices. That is we start with $A = (a_{i,j})$ and $B = (b_{i,j}) \in \mathrm{tri}_n^1(R)$ and need to show $AB \in \mathrm{tri}_n^1(R)$. We have just seen in the proof of (4.14) that the

(i,k)-th entry of AB is given by the following sum

$$\mathrm{ent}_{i,k}(AB) \;=\; \sum_{j=k}^{i} a_{i,j}b_{j,k}$$

and that thereby $AB \in \mathrm{tri}_n(R)$. It remains to verify, that AB only has 1 on its diagonal. But for $i = k$ this formula already turns into

$$\mathrm{ent}_{i,i}(AB) \;=\; a_{i,i}b_{i,i} \;=\; 1$$

Thus $AB \in \mathrm{tri}_n^1(R)$, as claimed. It remains to prove that A^{-1} is an element of $\mathrm{tri}_n^1(R)$ again. But we have already argued in (4.14) that $A^{-1} \in \mathrm{tri}_n(A)$. Again it remains to verify $\mathrm{ent}_{j,j}(A^{-1}) = 1$ for any $j \in 1 \ldots n$. As in the proof of (4.14) let x_j denote the j-th column of A^{-1} which amounts to $Ax_j = e_j$. In the case $j = n$ we have $[x_n]_n = a_{n,n}^{-1}[e_n]_n = 1$. For $j < n$ we start with $[x_j]_n = a_{n,n}^{-1}[e_j]_n = 0$. Then for any k with $j < k \leq n$ we use the recursion formula of (4.14) to prove that $[x_j]_k = 0$:

$$[x_j]_k \;=\; a_{k,k}^{-1}\left([e_j]_k - \sum_{l=k+1}^{n} a_{i,l}\cdot[x_j]_l\right) \quad 1\cdot(0-0) \;=\; 0$$

For $k = j$ however we get $[e_j]_j = 1$ and hence the same recursion formula yields 1 as $[x_j]_j = 1$ which is the (j,j)-th entry of A^{-1}. From this we get $A^{-1} \in \mathrm{tri}_n^1(R)$, as needed.

$$[x_j]_j \;=\; a_{j,j}^{-1}\left([e_j]_j - \sum_{l=j+1}^{n} a_{i,l}\cdot[x_j]_l\right) \quad 1\cdot(1-0) \;=\; 1$$

Altogether $\mathrm{tri}_n^1(R)$ is a subgroup of the multiplicative group $\mathrm{gl}_n(R)$. It remains to prove, that if A and B of the special form, described in the implications (1) and (2) then AB is a direct composite of A and B in the sense of the explicit formula for AB. We already know that $AB \in \mathrm{tri}_n^1(R)$ so we only have to regard the (i,k)-th entries with $i < k$. To see this we distinguish two separate cases: If $k > r$ then

$$\mathrm{ent}_{i,k}(AB) \;=\; \sum_{j=1}^{n} a_{i,j}b_{j,k} \;=\; a_{i,k}b_{k,k} + \sum_{j\neq k} a_{i,j}b_{j,k}$$

But as $k > r$ and $j \neq k$ we have $b_{j,k} = 0$ by assumption on B and $b_{k,k} = 1$ is granted, as well. And from this we get $\mathrm{ent}_{i,k}(AB) = a_{i,k}$ for any $k > r$. Alternatively, if $k \leq r$ we compute

$$\mathrm{ent}_{i,k}(AB) \;=\; \sum_{j=1}^{n} a_{i,j}b_{j,k} \;=\; a_{i,i}b_{i,k} + \sum_{j\neq i} a_{i,j}b_{j,k}$$

If $j \leq r$, then by assumption on A we have $a_{i,j} = 0$. If $j > r$, then $k \leq r < j$ implies $k < j$ and hence $b_{j,k} = 0$, as B is an upper triangular matrix. Altogether, with $a_{i,i} = 1$ this is $\mathrm{ent}_{i,k}(AB) = b_{i,k}$. And together this means, that AB is of the form given in the claim. □

Proof of (4.18):

(i) Let us denote $A = (a_{i,j}) \in \mathrm{mat}_{m,n}(R)$ and $B = b_{i,j} \in \mathrm{mat}_{n,m}(R)$. By definition we have $E_{r,s} =$

$(\delta_{i,r}\delta_{j,s})$, hence - for any $i, k \in 1 \ldots n$ we may simply compute the matrix multiplication

$$\mathrm{ent}_{i,k}(AE_{r,s}) \;=\; \sum_{j=1}^{n} a_{i,j}\delta_{j,r}\delta_{k,s} \;=\; a_{i,r}\delta_{k,s}$$

That is the (i,j)-th entry of $AE_{r,s}$ is zero, if $k \neq s$ and if $k = s$, then it simply is $a_{i,r}$. For the k-th column this implies

$$\mathrm{col}_k(AE_{r,s}) \;=\; \delta_{k,s}\,(a_{1,r},\ldots,a_{i,r}) \;=\; \delta_{k,s}\,\mathrm{col}_r(A)$$

Likewise we compute the (i,k)-th entry of $E_{r,s}B$ and use this to evaluate the i-th row of this matrix. This time we get

$$\mathrm{ent}_{i,k}(E_{r,s}B) \;=\; \sum_{j=1}^{n} \delta_{i,r}\delta_{j,s}b_{j,k} \;=\; \delta_{i,r}b_{s,k}$$

$$\mathrm{row}_i(E_{r,s}B) \;=\; \delta_{i,r}\,(b_{s,1},\ldots,b_{s,n}) \;=\; \delta_{i,r}\,\mathrm{row}_s(B)$$

(ii) This identity is a straightforward computation - just be aware that $\delta_{i,j}$ commutes with any other scalar of R and that the sum $\sum_j \delta_{i,j}x_j$ breaks down to x_i. Then we pick up any $p, s \in 1 \ldots n$ and compute

$$\begin{aligned}
\mathrm{ent}_{p,s}(E_{i,j}\,A\,E_{k,l}) &= \sum_{r=1} \mathrm{ent}_{p,r}(E_{i,j}\,A)\,\mathrm{ent}_{r,s}(E_{k,l}) \\
&= \sum_{r=1}\sum_{q=1}^{n} \mathrm{ent}_{p,q}(E_{i,j})\,a_{q,r}\,\mathrm{ent}_{r,s}(E_{k,l}) \\
&= \sum_{r=1}\sum_{q=1}^{n} \delta_{i,p}\,\delta_{j,q}\,a_{q,r}\,\delta_{k,r}\,\delta_{l,s} \\
&= \delta_{i,p}\,a_{j,k}\,\delta_{l,s} \;=\; a_{j,k}\,\mathrm{ent}_{p,s}(E_{i,l})
\end{aligned}$$

(iii) This is an ultimate consequence of (i): clearly $T_{r,s}B = (\mathbb{1}_n + aE_{r,s})B = B + aE_{r,s}B$. Hence the i-th row of $T_{r,s}(a)B$ is given to be

$$\begin{aligned}
\mathrm{row}_i(T_{r,s}(a)B) &= \mathrm{row}_i(B) + a\,\mathrm{col}_k(E_{r,s}B) \\
&= \mathrm{row}_i(B) + \delta_{k,s}\,a\,\mathrm{row}_i(B)
\end{aligned}$$

Likewise we have $AT_{r,s} = A(\mathbb{1}_n + aE_{r,s}) = A + (Aa)E_{r,s}$. And hence the k-th column of $AT_{r,s}(a)$ is given to be

$$\begin{aligned}
\mathrm{col}_k(AT_{r,s}(a)) &= \mathrm{col}_k(A) + \mathrm{col}_k((Aa)E_{r,s}) \\
&= \mathrm{col}_k(A) + \delta_{k,s}\,\mathrm{col}_r(Aa) \\
&= \mathrm{col}_k(A) + \delta_{k,s}\,\mathrm{col}_r(A)\,a
\end{aligned}$$

(iv) Let us denote $x_j = (x_{1,j},\ldots,x_{m,j}) \in R^m$, that is x_j is the j-th column of the matrix $X = x_{i,j} \in \mathrm{mat}_{m,n}(R)$. By definition the diagonal matrix $D := \mathrm{dia}(a_1,\ldots,a_n)$ has $\delta_{i,j}a_j$ as its (i,j)-th entry.

We begin by proving the second equality by simple matrix-multiplication

$$\mathrm{ent}_{i,k}(XD) \;=\; \sum_{j=1}^{n} x_{i,j}\delta_{j,k}a_k \;=\; x_{i,k}a_k$$

Therefore the k-th colums of XD is $\mathrm{col}_k(XD) = (x_{1,k}a_k, \ldots, x_{m,k}a_k)$ which is $x_k a_k$ as we had claimed. In the first equality the x_j are used as rows, that is we actually deal with the transpose X^* of X. Hence the correct ansatz is

$$\mathrm{ent}_{i,k}(DX^*) \;=\; \sum_{j=1}^{n} \delta_{i,j}a_j x_{k,j} \;=\; a_i x_{k,i}$$

Therefore the i-th row of X^* is $\mathrm{row}_i(DX^*) = (a_i x_{1,i}, \ldots, a_i x_{m,i})$ which is $a_i x_i$. Hence we also have shown the first equality.

(v) These equations are straightforward computations using the definition $N_n = (\delta_{i+1,j})$. Let us denote $x_j = (x_{1,j}, \ldots, x_{m,j}) \in R^m$, then $X = (x_{i,j})$ is the $(m \times n)$-matrix composed of the *columns* x_j. Hence the transposed matrix X^* has the *rows* x_j. Thereby for any $i, k \in 1 \ldots n$

$$\mathrm{ent}_{i,k}(XN_n) \;=\; \sum_{j=1}^{n} x_{i,j}\,\delta_{j+1,k} \;=\; \begin{cases} x_{i,k-1} \text{ if } k > 1 \\ 0 \text{ if } k = 1 \end{cases}$$

$$\mathrm{ent}_{i,k}(N_nX^*) \;=\; \sum_{j=1}^{n} \delta_{i+1,j}\,x_{k,j} \;=\; \begin{cases} x_{k,i+1} \text{ if } i < n \\ 0 \text{ if } i = n \end{cases}$$

Once the entries are established, it is easy to evaluate the rows and colums of these matrix products

$$\mathrm{col}_k(N_nX) \;=\; (x_{1,k-1}, \ldots, x_{m,k-1}) \;=\; \begin{cases} x_{k-1} \text{ if } k > 1 \\ 0 \text{ if } k = 1 \end{cases}$$

$$\mathrm{row}_i(N_nX^*) \;=\; (x_{1,i+1}, \ldots, x_{m,i+1}) \;=\; \begin{cases} x_{i+1} \text{ if } i < n \\ 0 \text{ if } i = n \end{cases}$$

(vi) Recall the definition of the permutation matrix $P_\sigma = (\delta_{\sigma(i),j})$. Let us denote $x_j = (x_{1,j}, \ldots, x_{m,j}) \in R^m$ and $X = (x_{i,j})$ again. Then the $(m \times n)$-matrix composed of the *columns* x_j and the transposed matrix X^* has the *rows* x_j. Thereby for any $i, k \in 1 \ldots n$

$$\mathrm{ent}_{i,k}(P_\sigma X^*) \;=\; \sum_{j=1}^{n} \delta_{\sigma(i),j}\,x_{k,j} \;=\; x_{k,\sigma(i)}$$

Hence the i-th row of $P_\sigma X^*$ is $(x_{1,\sigma(i)}, \ldots, x_{m,\sigma(i)})$ which is nothing but $x_{\sigma(i)}$. Now we supposed that σ is bijective, that is the equation $\sigma(j) = k$ has the unique solution $j = \sigma^{-1}(k)$. Then we get

$$\mathrm{ent}_{i,k}(XP_\sigma) \;=\; \sum_{j=1}^{n} x_{i,j}\,\delta_{\sigma(j),k} \;=\; x_{i,\sigma^{-1}(k)}$$

Thereby the k-th column of XP_σ is $(x_{1,\sigma^{-1}(k)}, \ldots, x_{m,\sigma^{-1}(k)})$ which nothing but $x_{\sigma^{-1}(k)}$. Altogether we have proved the equalities given.

□

Proof of (4.21):

(i) It is clear that the map given is an R-module homomorphism, as the operations are point-wise, in both cases. The bijectivity is trivial as well. As also $(1,\dots,1) \mapsto \mathrm{dia}(1,\dots,1) = \mathbb{1}_n$ it only remains to prove, that the map also transfers the respective multiplications. Hence consider any $a_1,\dots,a_n$ and $b_1,\dots,b_n \in R$. Using (4.18.(ii)) we find

$$\begin{aligned} & \mathrm{dia}(a_1,\dots,a_n)\,\mathrm{dia}(b_1,\dots,b_n) \\ = & \left(\sum_{i=1}^{n} a_i\,E_{i,i}\right)\left(\sum_{j=1}^{n} b_j\,E_{j,j}\right) \\ = & \sum_{i=1}^{n}\sum_{j=1}^{n} a_i\,b_j\,E_{i,i}\,E_{j,j} \\ = & \sum_{i=1}^{n}\sum_{j=1}^{n} a_i\,b_j\,\delta_{i,j}\,E_{i,j} \\ = & \sum_{i=1}^{n} a_i\,b_i\,E_{i,i} \;=\; \mathrm{dia}(a_1\,b_1,\dots,a_n\,b_n) \end{aligned}$$

That is we have shown that the map given truly is an isomorphism of R-algebras. Also $\mathrm{dia}(a_1,\dots,a_n)\,\mathrm{dia}(b_1,\dots,b$ $\mathbb{1}_n = \mathrm{dia}(1,\dots,1)$ is satisfied if and only if $a_ib_i = 1$ for any $i \in 1\dots n$. Likewise $b_ia_i = 1$ for any $i \in 1\dots n$. But this is equivalent to $a_i \in R^*$ being a unit in R with inverse $b_i = a_i^{-1}$. Hence $\mathrm{dia}(a_1,\dots,a_n)$ is invertible if and only $a_i \in R^*$ for any $i \in 1\dots n$.

(ii) This is just a special case of (i) - the i-th entry is fixed to be a and the other $n-1$ entries are 1, which always is a unit $1 \in R^*$ of R.

(iii) Using (4.18.(ii)) again, the multiplication property of the transposition matrices is an easy computation

$$\begin{aligned} T_{i,j}(a)\,T_{i,j} &= (\mathbb{1}_n + aE_{i,j})(\mathbb{1}_n + bE_{i,j}) \\ &= \mathbb{1}_n + (a+b)\,E_{i,j} + ab\,E_{i,j}^2 \\ &= \mathbb{1}_n + (a+b)\,E_{i,j} \\ &= T_{i,j}(a+b) \end{aligned}$$

Hereby $E_{i,j}^2 = 0$, as we have assumed $i \neq j$ to be distinct. Now, as $T_{i,j}(0) = \mathbb{1}_n$ we see that $T_{i,j}(a)T_{i,j}(-a) = \mathbb{1}_n$ and of course also $T_{i,j}(-a)T_{i,j}(a) = \mathbb{1}_n$. That is $T_{i,j}(a)$ is invertible and the inverse is given to be $T_{i,j}(-a)$.

(iv) Let $\mathcal{E} = \{\,e_1,\dots,e_n\,\}$ be the Euclidean basis of R^n. By definition of the permutation matrices the i-th row of P_τ is $x_i := e_{\tau(i)}$. We now use the multiplication formula (4.18.(vi)) for permutation matrices, then the i-th row of $P_\sigma P_\tau$ is $x_{\sigma(i)}$ and this is $e_{\tau(\sigma(i))}$ in turn. Altogether we find

$$P_\sigma\,P_\tau \;=\; P_\sigma \begin{pmatrix} — & e_{\tau(1)} & — \\ & \vdots & \\ — & e_{\tau(n)} & — \end{pmatrix} = \begin{pmatrix} — & e_{\tau\sigma(1)} & — \\ & \vdots & \\ — & e_{\tau\sigma(n)} & — \end{pmatrix} = P_{\tau\sigma}$$

Again it is clear that truly $P_{id} = \mathbb{1}_n$. Hence if σ is bijective, then $P_\sigma P_{\sigma^{-1}} = P_{id} = \mathbb{1}_n$ and analogously $P_\sigma^{-1} P_\sigma = P_{id} = \mathbb{1}_n$ such that P_σ is invertible and the inverse is given to be $P_{\sigma^{-1}}$. Conversely suppose $P_\sigma P_\tau = \mathbb{1}_n$ and $P_\tau P_\sigma = \mathbb{1}_n$. By comparing coefficients we find that $\tau\sigma = id$ and $\sigma\tau = id$, that is τ is the inverse function of σ and in particular σ is bijective.

It remains to prove that the transpose P_σ^* also is the inverse P_σ^{-1}. As P_σ has been defined in such a way, as $\mathrm{col}_i(P_\sigma) = e_{\sigma(i)}$ we find that the transpose of P_σ is given by $\mathrm{row}_i(P_\sigma^*) = e_{\sigma(i)}$. Then we can use (4.18.(vi)) again, to compute

$$\begin{aligned} P_\sigma^* P_\sigma &= \begin{pmatrix} | & | & & | \\ e_{\sigma(1)} & e_{\sigma(2)} & \cdots & e_{\sigma(n)} \\ | & | & & | \end{pmatrix} P_\sigma \\ &= \begin{pmatrix} | & | & & | \\ e_{\sigma^{-1}((\sigma(1))} & e_{\sigma^{-1}((\sigma(2))} & \cdots & e_{\sigma^{-1}((\sigma(n))} \\ | & | & & | \end{pmatrix} = \mathbb{1}_n \end{aligned}$$

And as we have already proved, that P_σ is invertible we can multiply the equation $P_\sigma^* P_\sigma = \mathbb{1}_n$ with P_σ^{-1} from the right to find

$$P_\sigma^* = P_\sigma^*(P_\sigma P_\sigma^{-1}) = (P_\sigma^* P_\sigma) P_\sigma^{-1} = P_\sigma^{-1}$$

(v) By associativity of the matrix multiplication we can evaluate $P_\varrho A$ first: But then P_ϱ permutes the rows of A, by (4.18.(vi)) and this is $P_\varrho A = (a_{\varrho(i),j})$. Multiplying $P_\sigma^{-1} = P_{\sigma^{-1}}$ from the right permutes the columns of this matrix yields and hence

$$P_\varrho A P_\sigma^{-1} = \big(P_\varrho A\big) P_{\sigma^{-1}} = \big(a_{\varrho(i),j}\big) P_{\sigma^{-1}} = \big(a_{\varrho(i),\sigma(j)}\big)$$

□

Proof of (4.40):

- Let $\mathcal{M} = (m_1, \ldots, m_s)$ be an ordered basis of M and consider a scalar $a \in R$ and two vectors $x = \sum_j x_j m_j$ and $y = \sum_j y_j m_j \in M$. Then it is clear, that $ax = \sum_j a x_j m_j$ and $x + y = \sum_j (x_j + y_j) m_j$ and thereby we get $[ax]_j = a x_j = a[x]_j$ and $[x+y]_j = x_j + y_j = [x]_j + [y]_j$. And as this is true for any $j \in 1 \ldots s$ and $[x]_\mathcal{M} = ([x]_1, \ldots, [x]_s)$ we conclude $[ax]_\mathcal{M} = a[x]_\mathcal{M}$ and $[x+y]_\mathcal{M} = [x]_\mathcal{M} + [y]_\mathcal{M}$.
- Likewise let $\mathcal{N} = (n_1, \ldots, n_r)$ be an ordered basis of N and consider two R-module-homomorphisms φ and $\psi : M \to N$. Let $A = (a_{i,j}) = [\varphi]_\mathcal{M}^\mathcal{N}$ and $B = (b_{i,j}) = [\psi]_\mathcal{M}^\mathcal{N}$ be the matrix representations of φ and ψ respectively. Then we compute

$$\begin{aligned} (a\varphi)(m_j) &= a\varphi(m_j) = a \sum_{i=1}^r a_{i,j} n_i = \sum_{i=1}^r a a_{i,j} n_i \\ (\varphi + \psi)(m_j) &= \varphi(m_j) + \psi(m_j) \\ &= \sum_{i=1}^r a_{i,j} n_i + \sum_{i=1}^r b_{i,j} n_i = \sum_{i=1}^r (a_{i,j} + b_{i,j}) n_i \end{aligned}$$

That is for any $j \in 1 \ldots s$ and any $i \in 1 \ldots r$ we find $[a\varphi]_{i,j} = a a_{i,j} = a[\varphi]_{i,j}$ and $[\varphi + \psi]_{i,j} =$

$a_{i,j} + b_{i,j} = [\varphi]_{i,j} + [\psi]_{i,j}$. And as this is true for any combination of i and j this yields to following identities for the matrices $[a\varphi]^{\mathcal{N}}_{\mathcal{M}} = a[\varphi]^{\mathcal{N}}_{\mathcal{M}}$ and $[\varphi + \psi]^{\mathcal{N}}_{\mathcal{M}} = [\varphi]^{\mathcal{N}}_{\mathcal{M}} + [\psi]^{\mathcal{N}}_{\mathcal{M}}$.

- Finally assume that R is commutative and let $\mathcal{L} = (\ell_1, \ldots, \ell_t)$ be an ordered basis of L and we consider $x \in L$ and the R-module-homomorphisms $\varphi : L \to M$ and $\psi : M \to N$. If now $[x]_{\mathcal{L}} = u = (u_1, \ldots, u_t)$ and $[\varphi]^{\mathcal{M}}_{\mathcal{L}} = A = (a_{j,k})$ and $[\psi]^{\mathcal{N}}_{\mathcal{M}} = B = (b_{i,j})$ are the respective basis representations, then we compute

$$\begin{aligned}
\varphi(x) &= \varphi\left(\sum_{k=1} u_k \ell_k\right) = \sum_{k=1}^{t} u_k \varphi(\ell_k) \\
&= \sum_{k=1}^{t} u_k \sum_{j=1}^{s} a_{j,k} m_j \\
&= \sum_{j=1}^{s} \left(\sum_{k=1}^{t} a_{j,k} u_k\right) m_j \\
&= \sum_{j=1}^{s} [Au]_j \, m_j
\end{aligned}$$

That is $[\varphi(x)]_j = [Au]_j$ and as this is true for any $j \in 1 \ldots s$ we have shown, that $[\varphi(x)]_{\mathcal{M}} = Au = [\varphi]^{\mathcal{M}}_{\mathcal{L}} [x]_{\mathcal{L}}$. In complete analogy

$$\begin{aligned}
\psi\varphi(\ell_k) &= \psi(\varphi(\ell_k)) = \psi\left(\sum_{j=1}^{s} a_{j,k} m_j\right) \\
&= \sum_{j=1}^{s} a_{j,k} \psi(m_j) = \sum_{j=1}^{s} a_{j,k} \sum_{i=1}^{r} b_{i,j} n_i \\
&= \sum_{i=1}^{r} \left(\sum_{j=1}^{s} b_{i,j} a_{j,k}\right) n_i = \sum_{i=1}^{r} [BA]_{i,k} \, n_i
\end{aligned}$$

That is we have found that the (i,k)-th coefficient of the matrix of $\psi\varphi$ is given to be $[\psi\varphi]_{i,k} = [\psi\varphi(\ell_k)]_i = [BA]_{i,k}$ and as this is true for any $i \in 1 \ldots r$ and $k \in 1 \ldots t$ this is $[\psi\varphi]^{\mathcal{N}}_{\mathcal{L}} = BA = [\psi]^{\mathcal{N}}_{\mathcal{M}} [\varphi]^{\mathcal{M}}_{\mathcal{L}}$.

- At last we take a look at the map $\varphi \mapsto A$, where $\varphi \in \mathrm{mhom}(M,N)$ and $A = [\varphi]^{\mathcal{N}}_{\mathcal{M}} \in \mathrm{mat}_{r,s}(R)$. We have shown already, the this is a homomorphism. It remains to verify, that it is bijective, more precisely that the inverse map is $A \mapsto \varphi_A$ [where φ_A has been defined in the claim (4.40]. For ease of notation let us fix $\mathcal{M}$ and $\mathcal{M}$, that is we abbreviate $[x] = [x]_{\mathcal{M}}$ for any $x \in M$, $[y] = [y]_{\mathcal{N}}$ for any $y \in N$ and $[\varphi] = [\varphi]^{\mathcal{N}}_{\mathcal{M}}$ for any $\varphi : M \to N$.

 In a first step we will show $\varphi \mapsto [\varphi] \mapsto \varphi_{[\varphi]} = \varphi$ for any $\varphi : M \to N$. But this is straightforward: By definition we have $[\varphi_A(x)] = A[x]$ for any $x \in M$ and thereby

$$\Big[\varphi_{[\varphi]}(x)\Big] = [\varphi][x] = [\varphi(x)]$$

 Since $\mathcal{N}$ is a basis of N it is clear, that $y \mapsto [y]$ is bijective, from which we find that $\varphi(x) = \varphi_{[\varphi]}(x)$ for any $x \in M$ and hence $\varphi = \varphi_{[\varphi]}$. Conversely for $A \mapsto \varphi_A \mapsto [\varphi_A] = A$ we first note, that

$[m_j] = e_j \in \mathcal{E}(s)$ is an Euclidean base vector. Thereby we get

$$\varphi_A(m_j) \;=\; \sum_{i=1}^{r} [Ae_j]_i \, n_i \;=\; \sum_{i=1}^{r} a_{i,j} \, n_i$$

That is $[\varphi_A(m_j)]_i = a_{i,j}$ and hence $[\varphi_A(m_j)] = \mathrm{col}_j(A)$. But as $[\varphi_A(m_j)]$ is the j-th column of $[\varphi_A]$ (refer to remark (4.36) for this) we have established $[\varphi_A] = A$. Thus $\varphi \mapsto [\varphi]$ has an inverse map (namely $A \mapsto \varphi_A$) and hence is bijective.

- It only remains to prove the correspondence of isomorphisms and invertible matrices: Fix the ordered bases $\mathcal{M} = (m_1, \ldots, m_s)$ and $\mathcal{N} = (n_1, \ldots, n_r)$ of M and N respectively, again. If φ is bijective, let us denote $A := [\varphi]^{\mathcal{N}}_{\mathcal{M}}$ and $B := [\varphi^{-1}]^{\mathcal{M}}_{\mathcal{N}}$. Then we have just seen, that

$$\mathbb{1}_s \;=\; [\mathbb{1}_M]^{\mathcal{M}}_{\mathcal{M}} \;=\; [\varphi^{-1}\varphi]^{\mathcal{M}}_{\mathcal{M}} \;=\; [\varphi^{-1}]^{\mathcal{M}}_{\mathcal{N}} \, [\varphi]^{\mathcal{N}}_{\mathcal{M}} \;=\; BA$$

That is we have $BA = \mathbb{1}_s$ and in complete analogy we find $AB = \mathbb{1}_r$. Together this is $B = A^{-1}$, as we had claimed. Conversely, if A is invertible, then we define $\psi : N \to M$ to be the homomorphism defined by A^{-1}, that is $\psi := \varphi_{A^{-1}}$. Then for any $x \in M$ we may compute

$$[\psi\varphi(x)]_{\mathcal{M}} \;=\; [\psi]^{\mathcal{M}}_{\mathcal{N}} \, [\varphi]^{\mathcal{N}}_{\mathcal{M}} \, [x]_{\mathcal{M}} \;=\; A^{-1} \, A \, [x]_{\mathcal{M}} \;=\; [x]_{\mathcal{M}}$$

This implies $\psi\varphi(x) = x$ and as x has been arbitrary, this is $\psi\varphi = \mathbb{1}_M$. In complete analogy we have $\varphi\psi = \mathbb{1}_N$ and therefore φ is bijective, with inverse map ψ.

□

Proof of (4.42):

(i) First of all it is clear, that $r = s$ is necessary for any of the statements: In (a) φ is an isomorphism and hence $r = \dim(M) = \dim(N) = s$ and in (b) and (c) only square matrices are invertible. Thus we may assume $r = s$ throughout the rest of the proof.

We start with (a) $\implies$ (c): Let $\mathcal{M} = (m_1, \ldots, m_s)$ and $\mathcal{N} = (n_1, \ldots, n_r)$ be ordered bases of M and N respectively. Then it is clear that $\mathbb{1}_s = [\mathbb{1}_M]^{\mathcal{M}}_{\mathcal{M}}$ since $\mathbb{1}_M(m_j) = m_j = \sum_i \delta_{i,j} m_i$ for any $j \in 1 \ldots s$. Now as $\varphi^{-1}\varphi = \mathbb{1}_M$ and $\varphi\varphi^{-1} = \mathbb{1}_N$ we may use (4.40) to compute

$$\mathbb{1}_s \;=\; [\mathbb{1}_M]^{\mathcal{M}}_{\mathcal{M}} \;=\; [\varphi^{-1}\varphi]^{\mathcal{M}}_{\mathcal{M}} \;=\; [\varphi^{-1}]^{\mathcal{N}}_{\mathcal{M}} \, [\varphi]^{\mathcal{M}}_{\mathcal{N}}$$

Thus if $A := [\varphi]^{\mathcal{M}}_{\mathcal{N}}$ and $B := [\varphi^{-1}]^{\mathcal{N}}_{\mathcal{M}}$ then we have $AB = \mathbb{1}_s$. But as we also find $BA = \mathbb{1}_r$ we see that A is invertible, with inverse matrix B. Hereby $BA = \mathbb{1}_r$ can be seen from

$$\mathbb{1}_r \;=\; [\mathbb{1}_N]^{\mathcal{N}}_{\mathcal{N}} \;=\; [\varphi\varphi^{-1}]^{\mathcal{N}}_{\mathcal{N}} \;=\; [\varphi]^{\mathcal{M}}_{\mathcal{N}} \, [\varphi^{-1}]^{\mathcal{N}}_{\mathcal{M}}$$

The implication (c) $\implies$ (b) is trivial: Note that by assumption on M and N there are some ordered bases $\mathcal{M}$ of M and $\mathcal{N}$ of N in the first place. So it only remains to verify (b) $\implies$ (a): Again let $A := [\varphi]^{\mathcal{M}}_{\mathcal{N}}$ and define $\psi : N \to M$ by virtue of $[\psi]^{\mathcal{N}}_{\mathcal{M}} = A^{-1}$ that is $\psi := \varphi_{A^{-1}}$ in the notation of (4.40). Then we compute

$$[\psi\varphi]^{\mathcal{M}}_{\mathcal{M}} \;=\; [\psi]^{\mathcal{N}}_{\mathcal{M}} \, [\varphi]^{\mathcal{M}}_{\mathcal{N}} \;=\; A^{-1}A \;=\; \mathbb{1}_s \;=\; [\mathbb{1}_M]^{\mathcal{M}}_{\mathcal{M}}$$

But as $\varphi \mapsto [\varphi]_{\mathcal{M}}^{\mathcal{M}}$ is bijective we find $\psi\varphi = \mathbb{1}_M$. In complete analogy we get $\varphi\psi = \mathbb{1}_n$ such that φ is bijective, with inverse map $\varphi^{-1} = \psi$.

(iii) We have to prove that $\mathcal{M}' := (m'_1, \ldots, m'_s)$ truly is an ordered basis of M. The cornerstone of this reasoning is the following computation for any $x = (x_1, \ldots, x_s) \in R^s$ take a look at

$$\begin{aligned}
\sum_{j=1}^{s} x_j\, m'_j &= \sum_{j=1}^{s} x_j \sum_{i=1}^{s} t_{i,j}\, m_i \\
&= \sum_{i=1}^{s} \left(\sum_{j=1}^{s} x_j\, t_{i,j} \right) m_i \\
&= \sum_{i=1}^{s} \left(\sum_{j=1}^{s} t_{i,j}\, x_j \right) m_i \\
&= \sum_{i=1}^{s} [Tx]_i\; m_i
\end{aligned}$$

Thus if we are given any $m \in M$ pick up some $y = (y_1, \ldots, y_s) \in R^s$ such that $m = \sum_i y_i m_i$. Then $x = (x_1, \ldots, x_s) := T^{-1}y \in R^s$ satisfies $[Tx]_i = y_i$ and hence $\sum_j x_j m'_j = \sum_i y_i m_i = m$. Thus for any $m \in M$ there is some $x \in R^s$ with $m = \sum_j x_j m'_j$ which means that $\{ m'_1, \ldots, m'_s \}$ generates M. But this set also is linearly independent: If $\sum_j x_j m'_j = 0$ then also $\sum_i [Tx]_i m_i = 0$, as these sums are equal. But as the m_i form a basis of M this means $[Tx]_i = 0$ for any $i \in 1 \ldots s$ and hence $Tx = 0$. But as T is invertible this can only happen if $x = 0$ such that $\{ m'_1, \ldots, m'_s \}$ also is linearly independent and hence a basis. Of course the m'_i thereby also are pairwise distinct, as $m'_i - m'_j = 0$ cannot occur for any $i \neq j \in 1 \ldots s$.

By construction of $\mathcal{M}'$ we have $\mathbb{1}_M(m'_j) = m'_j = \sum_i t_{i,j} m_i$. Therefore $[\mathbb{1}(m'_j)]_{\mathcal{M}} = (t_{1,j}, \ldots, t_{s,j}) = \mathrm{col}_j(T)$ such that $[\mathbb{1}_M]_{\mathcal{M}'}^{\mathcal{M}} = T$. Also $T\,[\mathbb{1}_M]_{\mathcal{M}}^{\mathcal{M}'} = [\mathbb{1}_M]_{\mathcal{M}'}^{\mathcal{M}} [\mathbb{1}_M]_{\mathcal{M}}^{\mathcal{M}'} = [\mathbb{1}_M]_{\mathcal{M}} = \mathbb{1}_n$ and likewise $[\mathbb{1}_M]_{\mathcal{M}}^{\mathcal{M}'}\, T = \mathbb{1}_n$. Together this implies $[\mathbb{1}_M]_{\mathcal{M}}^{\mathcal{M}'} = T^{-1}$.

(ii) Since $\mathbb{1}_M$ is invertible we already know that $[\mathbb{1}_M]_{\mathcal{M}}^{\mathcal{M}'}$ is invertible by (b) $\implies$ (a) in (i). Thus the implication (b) $\implies$ (a) of (ii) is just a special case of (i). To prove converse direction (a) $\implies$ (b) we start with *any* ordered basis $\mathcal{M}' = (m'_1, \ldots, m'_r)$ of M and define

$$m_j \;:=\; \sum_{i=1}^{s} a_{i,j}\, m'_i \;\in\; M$$

where $j \in 1 \ldots s$ and $A = (a_{i,j})$. As A is invertible, (iii) tells us, that $\mathcal{M} = (m_1, \ldots, m_s)$ is another ordered basis of M and that $[\mathbb{1}_M]_{\mathcal{M}}^{\mathcal{M}'} = A$ and this already is (b).

(iv) By (ii) we already know that $S = [\mathbb{1}_M]_{\mathcal{M}'}^{\mathcal{M}}$ and $T = [\mathbb{1}_N]_{\mathcal{N}}^{\mathcal{N}'}$ are invertible matrices. But as $\varphi = \mathbb{1}_N \varphi \mathbb{1}_M$ trivially is true, we may use (4.40) once again, to compute

$$[\varphi]_{\mathcal{M}'}^{\mathcal{N}'} \;=\; [\mathbb{1}_N \varphi \mathbb{1}_M]_{\mathcal{M}'}^{\mathcal{N}'} \;=\; [\mathbb{1}_N]_{\mathcal{N}}^{\mathcal{N}'} [\varphi]_{\mathcal{M}}^{\mathcal{N}} [\mathbb{1}_M]_{\mathcal{M}'}^{\mathcal{M}} \;=\; T[\varphi]_{\mathcal{M}}^{\mathcal{N}} S$$

(v) By (iv) we have $[\varphi]_{\mathcal{M}'} = T[\varphi]_{\mathcal{M}} S$ where $T = [\mathbb{1}_M]_{\mathcal{M}}^{\mathcal{M}'}$ and $S = [\mathbb{1}_M]_{\mathcal{M}'}^{\mathcal{M}}$. But by the same reasoning

as in (i) we find $S = T^{-1}$ due to

$$TS \;=\; [\mathbb{1}_M]^{\mathcal{M}'}_{\mathcal{M}}[\mathbb{1}_M]^{\mathcal{M}}_{\mathcal{M}'} \;=\; [\mathbb{1}_M]^{\mathcal{M}}_{\mathcal{M}} \;=\; \mathbb{1}_s$$

$$ST \;=\; [\mathbb{1}_M]^{\mathcal{M}'}_{\mathcal{M}}[\mathbb{1}_M]^{\mathcal{M}'}_{\mathcal{M}} \;=\; [\mathbb{1}_M]^{\mathcal{M}'}_{\mathcal{M}'} \;=\; \mathbb{1}_s$$

□

Proof of (4.45):

(i) Let us first prove that $\sim$ is an equivalence relation: First of all, we have $A \sim A$, since $A = \mathbb{1}_m A \mathbb{1}_n$. Also if $A \sim B$, that is $B = SAT$, then $A = S^{-1}BT^{-1}$ such that $B \sim A$. If $A \sim B$ and $C \in \mathrm{mat}_{m,n}(R)$ is another matrix, with $B \sim C$, that is $B = SAT$ and $C = UBV$ for some S, $U \in \mathrm{gl}_m(R)$ and some T, $V \in \mathrm{gl}_n(R)$, then $C = UBV = U(SAT)V = (US)A(TV)$. Thereby $US \in \mathrm{gl}_m(R)$ is invertible, with inverse $(US)^{-1} = S^{-1}U^{-1}$ and likewise $TV \in \mathrm{gl}_n(R)$ is invertible with inverse $(TV)^{-1} = V^{-1}T^{-1}$. That is $A \sim C$ such that all three properties of an equivalence relation are satisfied.

(i) In (i) we also claimed the equivalence of (a) $A \sim B$ and (b) $A = [\varphi]^{\mathcal{M}}_{\mathcal{N}}$ and $B = [\varphi]^{\mathcal{M}'}_{\mathcal{N}'}$ for some $\varphi : R^n \to R^m$. Thereby (b) $\implies$ (a) has already been proved in (4.42.(iii)). Conversely for (a) $\implies$ (b) we have $B = SAT$ for some $S \in \mathrm{gl}_m(R)$ and $T \in \mathrm{gl}_n(R)$. Now take $\varphi(x) := Ax$, $\mathcal{M}' := \mathcal{E}(m)$ the Euclidean basis of R^m and $\mathcal{N} := \mathcal{E}(n)$ the Euclidean basis of R^n. Further let $\mathcal{M} := S\mathcal{M}'$ and $\mathcal{N}' := T\mathcal{N}$. As $T : R^n \to R^n$ is an automorphism the image $\mathcal{N}'$ of $\mathcal{N}$ under T is an ordered basis of R^n again. Likewise $\mathcal{M}$ is an ordered basis of R^m. By construction it is clear, that

$$[\varphi]^{\mathcal{M}}_{\mathcal{N}} \;=\; [\varphi]^{\mathcal{E}(m)}_{\mathcal{E}(n)} \;=\; A$$

$$[\mathbb{1}]^{\mathcal{M}'}_{\mathcal{M}} \;=\; [\mathbb{1}]^{\mathcal{E}(m)}_{S\mathcal{E}(m)} \;=\; S$$

$$[\mathbb{1}]^{\mathcal{N}}_{\mathcal{N}'} \;=\; [\mathbb{1}]^{\mathcal{E}(n)}_{T\mathcal{E}(n)} \;=\; T$$

Therefore $B = SAT = [\mathbb{1}]^{\mathcal{N}}_{\mathcal{N}'}[\varphi]^{\mathcal{M}}_{\mathcal{N}}[\mathbb{1}]^{\mathcal{N}}_{\mathcal{N}'} = [\varphi]^{\mathcal{M}'}_{\mathcal{N}'}$ such that we have (b).

(ii) We will now prove that $\approx$ is an equivalence relation, as well: First of all, $A \approx A$ again, since $A = \mathbb{1}_n A \mathbb{1}_n^{-1}$. Also if $A \sim B$, that is $B = TAT^{-1}$ then $B = T^{-1}BT = T^{-1}B(T^{-1})^{-1}$. But as $T^{-1} \in \mathrm{gl}_n(R)$ again, this is $B \approx A$. If $A \approx B$ and $C \in \mathrm{mat}_n(R)$ is another matrix, with $B \approx C$, that is $B = TAT^{-1}$ and $C = UBU^{-1}$ for some T and $U \in \mathrm{gl}_n(R)$, then $C = UBU^{-1} = U(TAT^{-1})U^{-1} = (UT)A(T^{-1}U^{-1}) = (UT)A(UT)^{-1}$ and as $UT \in \mathrm{gl}_n(R)$ is invertible again, we find $A \approx C$ such that all three properties of an equivalence relation are satisfied.

(ii) In (ii) we also claimed the equivalence of (a) $A \approx B$ and (b) $A = [\varphi]_{\mathcal{M}}$ and $B = [\varphi]_{\mathcal{N}}$ for some $\varphi : R^n \to R^n$. Thereby (b) $\implies$ (a) has already been proved in (4.42.(v)). Conversely for (a) $\implies$ (b) we have $B = TAT^{-1}$ for some $T \in \mathrm{gl}_n(R)$. Analogous to (i) above, we let $\varphi(x) := Ax$ and $\mathcal{M} := \mathcal{E}(n)$ be the Euclidean basis of R^n. Now $\mathcal{N} := T^{-1}\mathcal{M}$, then it is clear, that

$$[\varphi]_{\mathcal{M}} \;=\; [\varphi]_{\mathcal{E}(n)} \;=\; A$$

$$[\mathbb{1}]_{\mathcal{N}}^{\mathcal{M}} \;=\; [\mathbb{1}]_{T^{-1}\mathcal{E}_{(n)}}^{\mathcal{E}_{(n)}} \;=\; T^{-1}$$

$$[\mathbb{1}]_{\mathcal{M}}^{\mathcal{N}} \;=\; \left([\mathbb{1}]_{\mathcal{N}}^{\mathcal{M}}\right)^{-1} \;=\; \left(T^{-1}\right)^{-1} \;=\; T$$

Therefore $B = TAT^{-1} = [\mathbb{1}]_{\mathcal{M}}^{\mathcal{N}}[\varphi]_{\mathcal{M}}[\mathbb{1}]_{\mathcal{N}}^{\mathcal{M}} = [\varphi]_{\mathcal{N}}$ such that (b) again.

(iii) By definition the image of B is the set of all $SATx$ where $x \in R^n$. As T is surjective we can take to $y := Tx \in \mathbb{R}^n$ and thereby compute

$$\begin{aligned}\operatorname{im}(B) \;&=\; \{\, SATx \mid x \in R^n \,\} \;=\; \{\, SAy \mid y \in R^n \,\} \\ &=\; S\,\{\, Ay \mid y \in R^n \,\} \;=\; S\operatorname{im}(A)\end{aligned}$$

By definition the kernel of B is the set of all $x \in \mathbb{R}^n$ such that $SATx = 0$. But as S is injective, this is equivalent to $ATx = 0$. Now let $y := Tx$ that is $x = T^{-1}y$, then we can compute

$$\begin{aligned}\operatorname{kn}(B) \;&=\; \{\, x \in R^n \mid SATx = 0 \,\} \;=\; \{\, x \in R^n \mid ATx = 0 \,\} \\ &=\; \left\{\, T^{-1}y \mid Ay = 0 \,\right\} \;=\; T^{-1}\operatorname{kn}(A)\end{aligned}$$

□

Proof of (4.46):

(i) By definition $\operatorname{ent}_{i,j}([\varphi]_{\mathcal{M}}) = [\varphi(m_j)]_i$. We consider any $j \le r$, if P is invariant under φ, then $\varphi(m_j) \in P = \operatorname{Lh}\{\, m_1, \ldots, m_r \,\}$ and hence the i-th coefficient in the basis representation of $\varphi(m_j)$ is 0, whenever $i > r$. This already is $A_{2,1} = 0$ and conversely, if $A_{2,1} = 0$ any $x \in P$ is mapped to $\varphi(x) \in \operatorname{Lh}\{\, m_1, \ldots, m_r \,\} = P$ again, such that $\varphi(P) \subseteq P$.

(ii) Let us abbreviate $A := [\varphi_1 \oplus \varphi_2]_{\mathcal{N}}^{\mathcal{M}}$ and $A_{k,k} = [\varphi_k]_{\mathcal{N}^k}^{\mathcal{M}^k}$ for $k = 1$ and $k = 2$. Then we have to show $A = A_{1,1} \oplus A_{2,2}$. In terms of (i) that is $A_{2,1} = 0$ and $A_{1,2} = 0$. But as $\varphi_1 \oplus \varphi_2(n_j^1, 0) = (\varphi_1(n_j^1), 0) \in N^1 \oplus 0$ we see that $N^1 \oplus 0$ is invariant under $\varphi_1 \oplus \varphi_2$ such that $A_{2,1} = 0$. Likewise $0 \oplus N^2$ is invariant under $\varphi_1 \oplus \varphi_2$ and in complete analogy this implies $A_{1,2} = 0$.

(iii) If $M = M_1 \oplus \cdots \oplus M_r$ then (as any M_i is free) choose bases $\mathcal{N}^i$ of M_i and let $\mathcal{N} := \mathcal{N}^1 \cup \cdots \cup \mathcal{N}^r$. Order $\mathcal{N}$ is such a way, that for $1 \le i < j \le r$ any $n_i \in M_i$ is in front of $n_j \in M_j$. The order inside $\mathcal{N}^i$ is irrelevant. As $\varphi(M_i) \subseteq M_i$ we may restrict φ to $\varphi_i : M_i \to M_i : x \mapsto \varphi(x)$. Now let $A_i := [\varphi_i]_{\mathcal{N}^i}$, then by (induction on) (ii) it is clear that $[\varphi]_{\mathcal{N}} = B := A_1 \oplus \cdots \oplus A_r$. As both $\mathcal{M}$ and $\mathcal{N}$ are bases of M, (4.42.(v)) implies $B = TAT^{-1}$ for $T = [\mathbb{1}]_{\mathcal{M}}^{\mathcal{N}}$, in particular $A \approx B$.

Conversely if $TAT^{-1} = B := A_1 \oplus \cdots \oplus A_r$ for some $T \in \mathrm{gl}_n(R)$, say $T^{-1} = (s_{i,j}) \in \mathrm{mat}_n(R)$. Recall that $\mathcal{M} = (m_1, \ldots, m_n)$ is a basis of M, then we define

$$b_j \;:=\; \sum_{i=1}^{n} s_{i,j} m_i \;\in\; M$$

As T^{-1} is invertible $\mathcal{B} := (b_1, \ldots, b_n)$ is another ordered basis of M, due to (4.42.(iii)) and we also get $T^{-1} = [\mathbb{1}]_{\mathcal{B}}^{\mathcal{M}}$ and likewise $T = [\mathbb{1}]_{\mathcal{M}}^{\mathcal{B}}$. But then B is the matrix representation of φ in $\mathcal{B}$, as

$$[\varphi]_{\mathcal{B}} \;=\; [\mathbb{1}]_{\mathcal{M}}^{\mathcal{B}}\,[\varphi]_{\mathcal{M}}\,[\mathbb{1}]_{\mathcal{B}}^{\mathcal{M}} \;=\; TAT^{-1} \;=\; B$$

Now define M_i (for $i \in 1 \dots r$) to be the sub-module of M generated by $b_{\ell(i)+1}$ to $b_{\ell(i)+k(i)}$ where $\ell(i) := k(1) + \cdots + k(i-1)$ and in particular $\ell(1) = 0$. That is

$$\begin{aligned} M_1 &:= \mathsf{Lh}\{\, b_j \mid 1 \le j \le k(1) \,\} \\ M_2 &:= \mathsf{Lh}\{\, b_j \mid k(1)+1 \le j \le k(1)+k(2) \,\} \\ &\vdots \qquad\quad \vdots \\ M_r &:= \mathsf{Lh}\{\, b_j \mid n-k(r)+1 \le j \le n \,\} \end{aligned}$$

By construction the M_i are free (as they are generated by linearly independent sets) and $M = M_1 \oplus \cdots \oplus M_r$ are we only partitioned the basis $\{\, b_1, \dots, b_n \,\}$ of M. But the M_i also are φ-invariant: For ease of notation take a look at $\varphi(b_1)$: Then

$$[\varphi(b_1)]_{\mathcal{B}} \;=\; [\varphi]_{\mathcal{B}}\,[b_1]_{\mathcal{B}} \;=\; B\,e_1 \;\in\; \mathsf{Lh}\{\, e_1, \dots, e_{k(1)} \,\}$$

Taking the preimage under the isomorphism $x \mapsto [x]_{\mathcal{B}}$ we hence get $\varphi(b_1) \in M_1$ again. In complete analogy we find $\varphi(b_j) \in M_i$ for any $b_j \in M_i$ and hence $\varphi(M_i) \subseteq M_i$. Altogether this is (a).

□

Proof of (4.47):
Let us denote the set of bilinear forms $M \oplus N \to R$ by $\mathrm{bil}(M \oplus N, R) := \{\, b : M \oplus N \to R \mid b \text{ is bilinear} \,\}$. Then we need to show the bijective correspondence of $\mathrm{bil}(M \oplus N, R) \longleftrightarrow \mathrm{mat}_{r,s}(R)$ under the maps given in the claim (4.47). To do this let us also denote the basis representations $u = (u_1, \dots, u_s) = [x]_{\mathcal{M}}$ of $x \in M$ and $v = (v_1, \dots, v_r) = [y]_{\mathcal{N}}$ of $y \in N$.
Let us start with a matrix $B = (b_{i,j}) \in \mathrm{mat}_{r,s}(R)$ then we assign the map $b : M \oplus N \to R$ by letting $b(x,y) := \langle Bu \mid v \rangle$. Since both maps $x \mapsto u = [x]_{\mathcal{M}}$ and $u \mapsto \langle Bu \mid v \rangle$ are R-linear so is their composition $x \mapsto \langle Bu \mid v \rangle$. But this is the linearity of b in the first argument. Likewise $y \mapsto v = [y]_{\mathcal{N}}$ and $v \mapsto \langle Bu \mid v \rangle$ are R-linear such that $y \mapsto \langle Bu \mid v \rangle$ is R-linear which is the linearity of b in the second argument. Altogether b is bilinear and $B \mapsto b$ is well-defined. Now an easy computation reveals

$$\begin{aligned} b(x,y) &= \langle Bu \mid v \rangle \;=\; \sum_{i=1}^{r} [Bu]_i\, v_i \\ &= \sum_{i=1}^{r} \left(\sum_{j=1}^{s} b_{i,j} u_j \right) v_i \\ &= \sum_{i=1}^{r} \sum_{j=1}^{s} b_{i,j} u_j v_i \end{aligned}$$

In particular we find $b(m_j, n_i) = b_{i,j}$ (for any $i \in 1 \dots r$ and $j \in 1 \dots s$) such that the converse map $\mathrm{bil}(M \oplus N, R) \to \mathrm{mat}_{r,s}(R)$ truly matches $b \mapsto B$ again. Conversely if we start with a bilinear map $b : M \oplus N \to R$ and assign the matrix $B = (b_{i,j})$ where $b_{i,j} = b(m_j, n_i)$ we may continue the above computation to find

$$\langle Bu \mid v \rangle \;=\; \sum_{i=1}^{r} \sum_{j=1}^{s} b_{i,j} u_j v_i \;=\; \sum_{i=1}^{r} \sum_{j=1}^{s} b(m_j, n_i) u_j v_i$$

$$= \; b\left(\sum_{j=1}^{s} u_j m_j, \sum_{i=1}^{r} v_i n_i\right) \; = \; b(x,y)$$

That is we have also found the opposite direction $B \mapsto b$. Altogether we have established the mutually inverse maps $b \mapsto B$ and $B \mapsto b$ such that the correspondence is proved. It remains to show that (under the assumptions $M = N$ and $\mathcal{M} = \mathcal{N}$) b is symmetric if and only if B is such. Well, if b is symmetric, then $b_{i,j} = b(m_j, m_i) = b_(m_i, m_j) = b_{j,i}$ is obvious. But the converse implication requires only little effort: if B is symmetric, then

$$b(x,y) \; = \; \langle Bu \mid v \rangle \; = \; \langle u \mid B^* v \rangle \; = \; \langle u \mid Bv \rangle \; = \; \langle Bv \mid u \rangle \; = \; b(y,x)$$

□

Proof of (2.34):

- (a) $\implies$ (b): we have the assumption of (ACC) and need to show, that there is some maximal element $\mathfrak{a}^* \in \mathcal{A}^*$. That is there has to be some $\mathfrak{a}^* \in \mathcal{A}$ such that $(\mathfrak{a}^* \subseteq \mathfrak{a}) \implies (\mathfrak{a}^* = \mathfrak{a})$ for any $\mathfrak{a} \in \mathcal{A}$. Yet this statement is logically equivalent, to saying

 $$\exists\, \mathfrak{a}^* \in \mathcal{A} \;\; \forall\, \mathfrak{a} \in \mathcal{A} \; : \; \neg(\mathfrak{a}^* \subseteq \mathfrak{a}) \vee (\mathfrak{a}^* = \mathfrak{a})$$

 Suppose this was not the case - that is the negation of this statement was true. This is $\forall\, \mathfrak{a}^* \in \mathcal{A}\, \exists\, \mathfrak{a} \in \mathcal{A}$ such that $(\mathfrak{a}^* \subseteq \mathfrak{a}) \wedge (\mathfrak{a}^* \neq \mathfrak{a})$. And clearly this means nothing but

 $$\forall\, \mathfrak{a}^* \in \mathcal{A} \;\; \exists\, \mathfrak{a} \in \mathcal{A} \; : \; \mathfrak{a}^* \subset \mathfrak{a}$$

 Thus we could start by picking up any one $\mathfrak{a}_1 \in \mathcal{A}$ as $\mathfrak{a}^*$. And by the above property there would be some $\mathfrak{a}_2 \in \mathcal{A}$ such that $\mathfrak{a}_1 \subset \mathfrak{a}_2$. Continuing this way (using induction with $\mathfrak{a}^* := \mathfrak{a}_k$ and $\mathfrak{a}_{k+1} := \mathfrak{a}$) we could construct an infinitely ascending chain if ideals $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots \subset \mathfrak{a}_k \subset \mathfrak{a}_{k+1} \subset \ldots$ in contradiction to (ACC). Hence the assumption has to be false and this means, that (b) holds true.

- (b) $\implies$ (c): For any subset $H \subseteq I$ with $H \neq \emptyset$ let us denote the ideal $\mathfrak{a}_H \trianglelefteq_{\mathfrak{i}} R$ and the set $\mathcal{A}$ of these ideals that found on a finite subset $H \subseteq I$ to be:

 $$\begin{aligned} \mathfrak{a}_H \;\; &:= \;\; \sum_{i \in H} \mathfrak{a}_i \\ \mathcal{A} \;\; &:= \;\; \{\, \mathfrak{a}_H \mid H \subseteq I, 1 \leq \#H < \infty \,\} \end{aligned}$$

 Clearly $\mathcal{A} \neq \emptyset$ is nonempty, as $\mathfrak{a}_i \in \mathcal{A}$ for any $i \in I$. Hence by assumption (b) $\mathcal{A}$ has a maximal element $\mathfrak{a}^*$ and say $\mathfrak{a}^* = \mathfrak{a}_\Omega$ for some finite $\Omega \subseteq I$. Now consider any $i \in I$, then $\mathfrak{a}^* \subseteq \mathfrak{a}^* + \mathfrak{a}_i$. But as $\mathfrak{a}^* + \mathfrak{a}_i = \mathfrak{a}_H$ for the finite set $H = \Omega \cup \{\, i \,\} \subseteq I$ and $\mathfrak{a}^*$ is maximal, we get $\mathfrak{a}^* = \mathfrak{a}^* + \mathfrak{a}_i$ and in particular $\mathfrak{a}_i \subseteq \mathfrak{a}^*$. As this is true for any $i \in I$ we have

 $$\bigcup_{i \in \mathfrak{a}_i} \;\; \subseteq \;\; \mathfrak{a}^* \;\; = \;\; \mathfrak{a}_\Omega$$

 But as $\mathfrak{a}_\Omega$ is an ideal of R, the same is true for the ideal generated by the union of the $\mathfrak{a}_i$. And by

definition this is nothing but

$$\sum_{i\in I}\mathfrak{a}_i \quad\subseteq\quad \mathfrak{a}_\Omega \quad=\quad \sum_{i\in\Omega}\mathfrak{a}_i$$

- (c) $\Longrightarrow$ (d): Consider any ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ and for any $a \in \mathfrak{a}$ we pick up the ideal $Ra \trianglelefteq_{\mathrm{i}} R$. Then

$$\sum_{a\in\mathfrak{a}} Ra \quad=\quad \mathfrak{a}$$

as any $Ra \subseteq \mathfrak{a}$ and conversely any $a \in \mathfrak{a}$ is contained in Ra. Also $\mathfrak{a} \neq \emptyset$, as $0 \in \mathfrak{a}$. Now by assumption (c) there is a finite subset $\{ a_1, \ldots, a_k \} \subseteq \mathfrak{a}$ such that

$$\sum_{a\in\mathfrak{a}} Ra \quad=\quad \sum_{i=1}^{k} Ra_i$$

and combining these equalities we have $\mathfrak{a} = Ra_1 + \cdots + Ra_k$. That is $\mathfrak{a}$ is finitely generated, which is claim (d) already.

- (d) $\Longrightarrow$ (a): consider an ascending chain $\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \ldots \subseteq \mathfrak{a}_k \subseteq \ldots$ of ideals in R. Then we define the set

$$\mathfrak{b} \qu:=\quad \bigcup_{k\in\mathbb{N}} \mathfrak{a}_k$$

As the $\mathfrak{a}_k$ have been a chain, we find that $\mathfrak{b} \trianglelefteq_{\mathrm{i}} R$ is an ideal due to (2.4.(i)). And hence by assumption (d) there are finitely many elements $a_1, \ldots, a_n \in R$ generating $\mathfrak{b} = \langle a_1, \ldots, a_n \rangle_{\mathrm{i}}$. So by construction of $\mathfrak{b}$ for any $i \in 1 \ldots n$ (as $a_i \in \mathfrak{b}$) there is some $s(i) \in \mathbb{N}$ such that $a_i \in \mathfrak{a}_{s(i)}$. Now let $s := \max\{ s(1), \ldots, s(n) \}$. Then for any $i \in 1 \ldots n$ and any $t \geq s$ we get $a_i \in \mathfrak{a}_{s(i)} \subseteq \mathfrak{a}_s \subseteq \mathfrak{a}_t$. In particular

$$\mathfrak{b} \;=\; \langle a_1, \ldots, a_n \rangle_{\mathrm{i}} \quad\subseteq\quad \mathfrak{a}_t \quad\subseteq\quad \mathfrak{b}$$

Of course this means $\mathfrak{b} = \mathfrak{a}_t$ for any $t \geq s$. And this is just another way of saying that the chain of the $\mathfrak{a}_k$ stabilized at level s.

By now we have proved the equivalence of (a) to (d) in the definition of noetherian rings. And trivially we also have (d) $\Longrightarrow$ (e). These are the most important equivalences, it merely is a neat fact that (e) also implies (d). Though we will not use it we wish to present a proof (note that this is substantially more complicated than the important implications above).

- We will now prove (e) $\Longrightarrow$ (d) in several steps: We want to prove that *any* ideal of R is finitely generated. Thus let us take the set of all those ideals of R *not* being finitely generated:

$$\mathcal{Z} \qu:=\quad \{\, \mathfrak{a} \trianglelefteq_{\mathrm{i}} R \mid \mathfrak{a} \text{ is } \textit{not} \text{ finitely generated} \,\}$$

The idea of the proof will then be the following: suppose $\mathcal{Z} \neq \emptyset$, then by an application of Zorn's lemma, there is some maxmal element $\mathfrak{p} \in \mathcal{Z}^*$. In a second step we will then prove that any $\mathfrak{p} \in \mathcal{Z}^*$ is prime. So by assumption (d) $\mathfrak{p}$ is finitely generated. But because of $\mathfrak{p} \in \mathcal{Z}$ it also is not finitely generated. This can only mean $\mathcal{Z} = \emptyset$ and hence any ideal of R is finitely generated. Thus it remains to prove:

- $\mathcal{Z} \neq \emptyset \implies \mathcal{Z}^* \neq \emptyset$: thus consider a chain $(\mathfrak{a}_i)$ (where $i \in I$) in $\mathcal{Z}$. Then we denote the union

of this chain by

$$\mathfrak{b} \;=\; \bigcup_{i\in I} \mathfrak{a}_i$$

By (2.4.(i)) $\mathfrak{b} \trianglelefteq_{\mathfrak{i}} R$ is an ideal of R again. Now suppose $\mathfrak{b} \notin \mathcal{Z}$, then $\mathfrak{b}$ would be finitely generated, say $\mathfrak{b} = \langle b, \ldots, b_n\rangle_{\mathfrak{i}}$. By construction of $\mathfrak{b}$ for any $k \in 1 \ldots n$ (as $b_k \in \mathfrak{b}$) there is some $i(k) \in I$ such that $b_k \in \mathfrak{a}_{i(k)}$. And as the $\mathfrak{a}_i$ form a chain we may choose $i \in I$ such that $\mathfrak{a}_i := \max\Big\{ \mathfrak{a}_{i(1)}, \ldots, \mathfrak{a}_{i(n)} \Big\}$. Thereby $\mathfrak{b} = \langle b_1, \ldots, b_n\rangle_{\mathfrak{i}} \subseteq \mathfrak{a}_i \subseteq \mathfrak{b}$. That is $\mathfrak{a}_i = \langle b_1, \ldots, b_n\rangle_{\mathfrak{i}}$ would be finitely generated in contradiction to $\mathfrak{a}_i \in \mathcal{Z}$. Thus we have $\mathfrak{b} \in \mathcal{Z}$ again and hence $\mathfrak{b}$ is an upper bound of $(\mathfrak{a}_i)$. Now - as any chain has an upper bound, by the lemma of Zorn - there is some maximal element $\mathfrak{p} \in \mathcal{Z}^*$.

- $\mathfrak{p} \in \mathcal{Z}^* \implies \mathfrak{p}$ prime: First note thet $\mathfrak{p} \neq R$, as $R = 1R$ is finitely generated. Now suppose $\mathfrak{p}$ was not prime, then there would be some $f, g \in R$ such that $f \notin \mathfrak{p}$, $g \notin \mathfrak{p}$ but $fg \in \mathfrak{p}$. Now let $\mathfrak{a} := \mathfrak{p} + fR$, as $f \notin \mathfrak{p}$ we find $\mathfrak{p} \subset \mathfrak{a}$. And as $\mathfrak{p}$ is a maximal element of $\mathcal{Z}$ this means that $\mathfrak{a}$ is finitely generated, say $\mathfrak{a} = \langle a_1, \ldots, a_k\rangle_{\mathfrak{i}}$. As the $a_i \in \mathfrak{a} = \mathfrak{p} + fR$ there are some $p_i \in \mathfrak{p}$ and $b_i \in R$ such that $a_i = p_i + fb_i$. Therefore

$$\mathfrak{a} \;=\; \langle p_1, \ldots, p_k, f\rangle_{\mathfrak{i}} \;=\; p_1R + \cdots + p_kR + fR$$

The inclusion " $\supseteq$ " is clear, as $p_i \in \mathfrak{p} \subseteq \mathfrak{a}$ and $f \in \mathfrak{a}$. Conversely consider $x \in \mathfrak{a}$, that is there are some $x_i \in R$ such that $x = \sum_i x_i a_i = \sum_i x_i p_i + f \sum_i x_i b_i \in p_1R + \cdots + p_kR + fR$. Next we note that

$$\mathfrak{p} \;=\; f(\mathfrak{p} : f) + p_1R + \cdots + p_kR$$

where $f(\mathfrak{p} : f) = (fR)\,(\mathfrak{p} : f) = \{\, fb \mid b \in \mathfrak{p} : f \,\} \trianglelefteq_{\mathfrak{i}} R$. The inclusion " $\supseteq$ " is easy: $p_i \in \mathfrak{p}$ is true by definition. Thus consider any element $x \in f(\mathfrak{p} : f)$. That is $x = fb$ for some $b \in \mathfrak{p} : f = \{\, b \in R \mid fb \in \mathfrak{p} \,\}$. In particular $x = bf \in \mathfrak{p}$, too. For the converse inclusion we are given any $q \in \mathfrak{p} \subseteq \mathfrak{a}$. That is there are some $x_i \in R$ and $y \in R$ such that $q = x_1p_1 + \cdots + x_kp_k + yf$. As q and all the p_i are contained in $\mathfrak{p}$ this implies $yf \in \mathfrak{p}$ and thereby $y \in \mathfrak{p} : f$. Thus $yf \in f(\mathfrak{p} : f)$ and hence $q \in p_1R + \cdots + p_kR + f(\mathfrak{p} : f)$. Finally we prove

$$\mathfrak{p} : a \;\notin\; \mathcal{Z}$$

Clearly we get $\mathfrak{p} \subseteq \mathfrak{p} : a$ and $b \in \mathfrak{p} : a$ (because of $ab \in \mathfrak{p}$). But $b \notin \mathfrak{p}$ and hence $\mathfrak{p} \subset \mathfrak{p} : a$. But by the maximality of $\mathfrak{p}$ in $\mathcal{Z}$ this means $\mathfrak{p} : a \notin \mathcal{Z}$. Thus $\mathfrak{p} : a$ is finitely generated and hence $a(\mathfrak{p} : a)$ is finitely generated, too. But as the sum of finitely generated ideals is finitely generated by (1.59) this means that $\mathfrak{p} = a(\mathfrak{p} : a) + p_1R + \cdots + p_k$ is finitely generated, too, in contradiction to $\mathfrak{p} \in \mathcal{Z}$. Thus the assumption of $\mathfrak{p}$ not being prime is false.

□

Proof of (2.40):

(i) We will only prove the noetherian case - the arinian case is an analogous argument involving descending (instead of ascending) chains of ideals. Thus consider an ascending chain of ideals in $R/\mathfrak{a}$

$$\mathfrak{u}_0 \;\subseteq\; \mathfrak{u}_1 \;\subseteq\; \ldots \;\subseteq\; \mathfrak{u}_k \;\subseteq\; \ldots \;\trianglelefteq_{\mathfrak{i}}\; R\Big/_{\mathfrak{a}}$$

By the correspondence theorem (1.66) the ideals $\mathfrak{u}_k$ are of the form $\mathfrak{u}_k = \mathfrak{b}_k/\mathfrak{a}$ for sufficient ideals $\mathfrak{b}_k := \varrho^{-1}(\mathfrak{u}_k) \trianglelefteq_{\mathrm{i}} R$. Now suppose $b \in \mathfrak{b}_k$ then $b + \mathfrak{a} \in \mathfrak{u}_k \subseteq \mathfrak{u}_{k+1} = \mathfrak{b}_{k+1}/\mathfrak{a}$ and hence $b \in \mathfrak{b}_{k+1}$ again. Thus we have found an ascending chain of ideals in R

$$\mathfrak{b}_0 \subseteq \mathfrak{b}_1 \subseteq \ldots \subseteq \mathfrak{b}_k \subseteq \ldots \trianglelefteq_{\mathrm{i}} R$$

As R is noetherian this chain has to be eventually constant, that is there is some $s \in \mathbb{N}$ such that for any $i \in \mathbb{N}$ we get $\mathfrak{b}_{s+i} = \mathfrak{b}_s$. But this clearly implies $\mathfrak{u}_{s+i} = \mathfrak{u}_s$ as well and hence $R/\mathfrak{a}$ is noetherian again.

(ii) If $\varphi : R \twoheadrightarrow S$ is a surjective homomorphism, then by the first isomorphism theorem (1.83) we get $R/\mathrm{kn}(\varphi) \cong_{\mathrm{r}} S$. But by assumption R is $\star$ and hence $R/\mathrm{kn}(\varphi)$ is $\star$, too, due to (i). And because of this isomorphy we find that S thereby is $\star$, as well [this is clear by transferring a chain of ideals from S to $R/\mathrm{kn}(\varphi)$ and returning to S].

(iii) First suppose that $R \oplus S$ is $\star$. Trivially we have the following surjective ring homomorphisms $R \oplus S \twoheadrightarrow R : (a,b) \mapsto a$ and $R \oplus S \twoheadrightarrow R : (a,b) \mapsto b$. Thus both R and S are $\star$ due to (ii). Conversely suppose both R and S are noetherian. We will prove that this implies $R \oplus S$ to be noetherian again (the proof in the artinian case is completely analogous). Thus consider an ascending chain of ideals of $R \oplus S$

$$\mathfrak{u}_0 \subseteq \mathfrak{u}_1 \subseteq \ldots \subseteq \mathfrak{u}_k \subseteq \ldots \trianglelefteq_{\mathrm{i}} R \oplus S$$

Clearly $R \oplus 0$ and $0 \oplus S \trianglelefteq_{\mathrm{i}} R \oplus S$ are ideals of $R \oplus S$, too. Thus we obtain ideals $\mathfrak{a}_k := \mathfrak{u}_k \cap (R \oplus 0)$ and $\mathfrak{b}_k := \mathfrak{u}_k \cap (0 \oplus S) \trianglelefteq_{\mathrm{i}} R \oplus S$ be intersection. And for these we get

$$\mathfrak{u}_k = \mathfrak{a}_k + \mathfrak{b}_k$$

The inclusion " $\supseteq$ " is clear, as $\mathfrak{a}_k$, $\mathfrak{b}_k \subseteq \mathfrak{u}_k$. For the converse inclusion "$\subseteq$" we are given some $(a,b) \in \mathfrak{u}_k$. As $\mathfrak{u}_k$ is an ideal we find $(a,0) = (1,0)(a,b)$ and $(0,b) = (0,1)(a,b) \in \mathfrak{u}_k$. And as also $(a,0) \in R \oplus 0$ and $(0,b) \in 0 \oplus S$ this yields $(a,b) = (a,0) + (0,b) \in \mathfrak{a}_k + \mathfrak{b}_k$. But as $\mathfrak{a}_k$ is an ideal of $R \oplus S$ contained in $R \oplus 0$ it in particular is an ideal of $\mathfrak{a}_k \trianglelefteq_{\mathrm{i}} R \oplus 0$. But clearly R and $R \oplus 0$ are isomorphic under $R \cong_{\mathrm{r}} R \oplus 0 : a \mapsto (a,0)$. Thus $\mathfrak{a}_k$ corresponds to the following ideal $\mathfrak{a}_k^\circ := \{\, a \in R \mid (a,0) \in \mathfrak{a}_k \,\} \trianglelefteq_{\mathrm{i}} R$. And thus we have found an ascending chain of ideals in R

$$\mathfrak{a}_0^\circ \subseteq \mathfrak{a}_1^\circ \subseteq \ldots \subseteq \mathfrak{a}_k^\circ \subseteq \ldots \trianglelefteq_{\mathrm{i}} R$$

Yet as R was assumed to be noetherian there is some $p \in \mathbb{N}$ such that for any $i \in \mathbb{N}$ we get $\mathfrak{a}_{p+i}^\circ = \mathfrak{a}_p^\circ$. And returning to $R \oplus 0$ (via $\mathfrak{a}_k = \{\, (a,0) \mid a \in \mathfrak{a}_k^\circ \,\}$) we find that $\mathfrak{a}_{p+i} = \mathfrak{a}_p$ as well. With the same argument for the $\mathfrak{b}_k$ we find some $q \in \mathbb{N}$ such that for any $i \in \mathbb{N}$ we get $\mathfrak{b}_{q+i} = \mathfrak{b}_q$. Now let $s := \max\{\, p, q \,\}$ then it is clear that for any $i \in \mathbb{N}$ we get

$$\mathfrak{u}_{s+i} = \mathfrak{a}_{s+i} + \mathfrak{b}_{s+i} = \mathfrak{a}_s + \mathfrak{b}_s = \mathfrak{u}_s$$

that is the chain of the $\mathfrak{u}_k$ has been eventually constant. And this means nothin but $R \oplus S$ being noetherian again.

□

Proof of (2.42):
This proof requires some working knowledge of polynomials as it is presented in sections 7.2 and 7.3. Yet as the techniques used in this proof are fairly easy to see we chose to place the proof here already. In case you encounter problems with the arguements herein refer to these sections first.

(1) In a first step let us consider the case where $S = R[t]$ is the polynomial ring over R. Thus consider an ideal $\mathfrak{u} \trianglelefteq_{\mathfrak{i}} S$, then we want to verify that $\mathfrak{u}$ is finitely generated. The case $\mathfrak{u} = 0$ is clear, thus we assume $\mathfrak{u} \neq 0$. Then for any $k \in \mathbb{N}$ we denote

$$\mathfrak{a}_k \;:=\; \{\, \mathrm{lc}(f) \mid f \in \mathfrak{u},\ \deg(f) = k \,\} \cup \{0\}$$

where $\mathrm{lc}(f) := f[\deg(f)]$ denotes the *leading coefficient* of f. We will first prove that $\mathfrak{a}_k \trianglelefteq_{\mathfrak{i}} R$ is an ideal of R: $0 \in \mathfrak{a}_k$ is clear by construction. Thus suppose $a, b \in \mathfrak{a}_k$ say $a = \mathrm{lc}(f)$ and $b = \mathrm{lc}(g)$. As both f and g are of degree k we get $(f+g)[k] = f[k] + g[k] = \mathrm{lc}(f) + \mathrm{lc}(g) = a + b$. Thus if $a + b = 0$ then $a + b \in \mathfrak{a}_k$ is clear. And else, if $a + b \neq 0$ then $f + g$ is of degree k, too and $\mathrm{lc}(f+g) = (f+g)[k] = a + b$. And as $f + g \in \mathfrak{u}$ again we find $a + b \in \mathfrak{a}_k$ in both cases. Now let $r \in R$ be any element, if $ra = 0$ then $ra \in \mathfrak{a}_k$ is trivial again. And else $rf : k \mapsto rf[k]$ is of degree k again and satisfies $\mathrm{lc}(rf) = (rf)[k] = r(f[k]) = r\mathrm{lc}(f) = ra$. And as also $rf \in \mathfrak{u}$ we again found $ra \in \mathfrak{a}_k$ in both cases. Altogether $\mathfrak{a}_k \trianglelefteq_{\mathfrak{i}} R$ is an ideal. Next we will also prove the containment $\mathfrak{a}_k \subseteq \mathfrak{a}_{k+1}$. That is we consider some $a = \mathrm{lc}(f) \in \mathfrak{a}_k$ again. As $f \in \mathfrak{u}$ we also have $tf : k \mapsto f[k-1] \in \mathfrak{u}$. Obviously $\deg(tf) = \deg(f) + 1 = k + 1$ and $\mathrm{lc}(tf) = f[k+1] = f[k] = a$. Thus we have found $a = \mathrm{lc}(tf) \in \mathfrak{a}_{k+1}$. Altogether we have found the following ascending chain of ideals of R

$$\mathfrak{a}_0 \;\subseteq\; \mathfrak{a}_1 \;\subseteq\; \ldots \;\subseteq\; \mathfrak{a}_k \;\subseteq\; \ldots \;\trianglelefteq_{\mathfrak{i}}\; R$$

- As R is noetherian this chain has to be eventually constant, that is there is some $s \in \mathbb{N}$ such that for any $i \in \mathbb{N}$ we get $\mathfrak{a}_{s+i} = \mathfrak{a}_s$. And furthermore any $\mathfrak{a}_k$ is finitely generated (as R is noetherian). As we may choose generators of $\mathfrak{a}_k$ we do so

$$\mathfrak{a}_k \;=\; \langle a_{k,1}, \ldots, a_{k,n(k)} \rangle_{\mathfrak{i}}$$

and pick up polynomials $f_{k,i} \in \mathfrak{u}$ of degree $\deg(f_{k,i}) = k$ such that $\mathrm{lc}(f_{k,i}) = a_{k,i}$. Then we define the following ideal of S

$$\mathfrak{w} \;:=\; \langle f_{k,1} \mid k \in 0 \ldots s,\ i \in 1 \ldots n(k) \rangle_{\mathfrak{i}}$$

- For the first step it remains to prove that $\mathfrak{u} = \mathfrak{w}$. Then $\mathfrak{u}$ is finitely generated, as we have given a list of generators explictly. The inclusion $\mathfrak{w} \subseteq \mathfrak{u}$ is clear, as any $f_{i,k} \in \mathfrak{u}$. For the converse inclusion we start with some $f \in \mathfrak{u}$ and need to show $f \in \mathfrak{w}$. This will be done by induction on the degree $k := \deg(f)$ of f. The case $f = 0$ is clear. If $\deg(f) = k = 0$ then $f \in R$ is constant, that is $f = \mathrm{lc}(f) \in \mathfrak{a}_0 = \langle a_{0,1}, \ldots, a_{0,n(0)} \rangle_{\mathfrak{i}} \subseteq \mathfrak{w}$. Thus for the induction step we suppose $k \geq 1$ and let $a := \mathrm{lc}(f) = f[k]$. If $k \leq s$ then $a \in \mathfrak{a}_k = \langle a_{k,1}, \ldots, a_{k,n(k)} \rangle_{\mathfrak{i}}$. That is there are some $b_i \in R$

such that $a = \sum_i a_{k,i} b_i$. Now let us define the polynomial

$$g \;:=\; \sum_{i=1}^{n(k)} b_i f_{k,i} \;\in\; \mathfrak{w}$$

Then it is clear that $\mathrm{lc}(g) = \sum_i b_i \mathrm{lc}(f_{i,k}) = a = \mathrm{lc}(f)$ and hence $\deg(f-g) < k$. Thus by the induction hypothesis we get $d := f - g \in \mathfrak{w}$ again and hence $f = d + g \in \mathfrak{w}$, too. It remains to check the case $k > s$. Yet this can be dealt with using a similar argument. As $k \geq s$ we have $a \in \mathfrak{a}_k = \mathfrak{a}_s$. That is $a = \sum_i a_{k,i} b_i$ for sufficient $b_i \in R$. This time

$$g \;:=\; \sum_{i=1}^{n(s)} b_i t^{k-s} f_{k,i} \;\in\; \mathfrak{w}$$

Then $\mathrm{lc}(g) = \sum_i b_i \mathrm{lc}(f_{i,k}) = a = \mathrm{lc}(f)$ again and as before this is $\deg(f-g) < k$. By induction hypothesis again $d := f - g \in \mathfrak{w}$ and hence $f = d + g \in \mathfrak{w}$. Thus we have finished the case $S = R[t]$.

(2) As a second case let us regard $S = R[t_1, \ldots, n]$ the polynomial ring in finitely many variables. Again we want to prove that S in noetherian, and this time we use induction on the number n of variables. The case $n = 1$ has just been treated in (1). Thus consider $R[t_1, \ldots, t_n, t_{n+1}]$. Then we use the isomorphy

$$R[t_1, \ldots, t_n, t_{n+1}] \;\cong_{\mathrm{r}}\; R[t_1, \ldots, t_n][t_{n+1}]$$
$$\sum_\alpha f[\alpha] t^\alpha \;\mapsto\; \sum_{i=0}^{\infty} \left(\sum_{\alpha_{n+1}=i} f[\alpha] t_1^{\alpha_1} \ldots t_n^{\alpha_n} \right) t_{n+1}^i$$

By induction hypothesis $R[t_1, \ldots, t_n]$ is noetherian already. And by (1) this implies $R[t_1, \ldots, t_n][t_{n+1}]$ to be noetherian, too. And using the above isomorphy we finally find that $R[t_1, \ldots, t_n, t_{n+1}]$ is noetherian.

(3) We now easily derive the the general claim: let S be finitely generated over R. That is there are finitely many $e_1, \ldots, e_n \in S$ such that $S = R[e_1, \ldots, e_n]$. Then we trivially have a surjective homomoprphism $R[t_1, \ldots, t_n] \twoheadrightarrow S : f \mapsto f(e_1, \ldots, e_n)$ form the polynomial ring onto S. And by (2.40.(iii)) this implies that S is noetherian, too.

□

Proof of (2.47):
Let us denote the prime ring of R by $P := \langle \emptyset \rangle_{\mathrm{r}}$. This is the image of the uniquely determined ring-homomorphism from $\mathbb{Z}$ to R (induced by $1 \mapsto 1$). That is $P = \mathrm{im}(\mathbb{Z} \to R)$ and in particular P is noetherian by (2.40.(ii)). Let us now denote the set of finite, non-empty subsets of R by I

$$I \;:=\; \{\, i \subseteq R \mid i \neq \emptyset,\, \#i < \infty \,\}$$

And for any $i \in I$ let us denote $R_i := P[i]$ the P-subalgebra of R generated by i. Then by the Hilbert's basis theorem R_i is noetherian as well. Given any $a \in R$ we clearly have $i := \{a\} \in I$ and $a \in R_i$. In particular the R_i cover R. And given any two $i, j \in I$ we have $k := i \cup j \in I$, too. We now claim that $R_i \cup R_j \subseteq R_i$: thus suppose $i = \{i_1, \ldots, i_n\}$ and let $a = f(i_1, \ldots, i_n)$ for some

polynomial $f \in P[t_1,\ldots,t_n]$. Then it is clear that $a = g(i_1,\ldots,i_n,j_1,\ldots,j_m) \in P[i \cup j] = R_k$ if we only let $g(t_1,\ldots,t_n,t_{n+1},\ldots,t_{n+m}) := f(t_1,\ldots,t_n) \in P[t_1,\ldots,t_{n+m}]$. Thus we have seen $R_i \subseteq R_k$ and $R_j \subseteq R_k$ can be proved in complete analogy. □

Proof of (2.45):

(i) This has been proved in (2.34) as implication (a) $\implies$ (b) already. The reader is asked to refer to page 1031 for the proof.

(iii) Just let $\mathcal{P} := \{\, \mathfrak{b} \in \operatorname{Spec}(R) \mid \mathfrak{p} \subseteq \mathfrak{b} \subset \mathfrak{q} \,\}$. Then $\mathcal{P} \neq \emptyset$ is non-empty, as $\mathfrak{p} \in \mathcal{P}$. But as we have seen (i) this already implies that there is some maximal element $\mathfrak{q}_\circ \in \mathcal{P}^*$.

(iv) For any ideal $R \neq \mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ let us denote $\mathbb{V}(\mathfrak{a}) := \{\, \mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{a} \subseteq \mathfrak{p} \,\}$ and $n(\mathfrak{a}) := \#\mathbb{V}(\mathfrak{a})_* \in \mathbb{N} \cup \{\infty\}$. That is $n(\mathfrak{a})$ is the number of minimal prime ideals lying over $\mathfrak{a}$. By (2.18.(iii)) we know $1 \leq n(\mathfrak{a})$. Now let

$$\mathcal{A} \;:=\; \{\, \mathfrak{a} \trianglelefteq_{\mathrm{i}} R \mid n(\mathfrak{a}) = \infty \,\}$$

be the set of all ideals having infinitely many minimal primes lying over it. We want to show that $\mathcal{A} = \emptyset$. Hence assume $\mathcal{A} \neq \emptyset$, then - by (i), as R is noetherian - we may choose some maximal ideal $\mathfrak{u} \in \mathcal{A}^*$ in $\mathcal{A}$. Clearly $\mathfrak{u}$ cannot be prime: if it was then $\mathfrak{u}$ would be contained in precisely one minimal prime - namely $\mathfrak{u}$ itself, that is $\mathbb{V}(\mathfrak{u})_* = \{\mathfrak{u}\}$. In particular we had $n(\mathfrak{u}) = 1 < \infty$ which contradicts $\mathfrak{u} \in \mathcal{A}$. Now, as $\mathfrak{u}$ is *not* prime, there are some $a, b \in R$ such that $ab \in \mathfrak{u}$ but $a, b \notin \mathfrak{u}$. Then we define the respective ideals

$$\mathfrak{a} \;:=\; \mathfrak{u} + aR \quad \text{and} \quad \mathfrak{b} \;:=\; \mathfrak{u} + bR$$

As $a \notin \mathfrak{u}$ we have $\mathfrak{u} \subset \mathfrak{a}$ and hence $\mathfrak{a} \notin \mathcal{A}$ due to the maximality of $\mathfrak{u}$. Likewise $\mathfrak{b} \notin \mathcal{A}$ and this means that $n(\mathfrak{a}), n(\mathfrak{b}) < \infty$ are finite. But we will now prove

$$\mathbb{V}(\mathfrak{u})_* \;\subseteq\; \mathbb{V}(\mathfrak{a})_* \cup \mathbb{V}(\mathfrak{b})_*$$

To see this let $\mathfrak{p} \in \mathbb{V}(\mathfrak{u})_*$ be a minimal prime ideal over $\mathfrak{u}$. If $a \in \mathfrak{p}$ then $\mathfrak{a} \subseteq \mathfrak{p}$. Else suppose $a \notin \mathfrak{p}$ then $ab \in \mathfrak{u} \subseteq \mathfrak{p}$ implies $b \in \mathfrak{p}$, as $\mathfrak{p}$ is prime. And thereby we get $\mathfrak{b} \subseteq \mathfrak{p}$. In any case $\mathfrak{p}$ lies over one of the ideals $\mathfrak{a}$ or $\mathfrak{b}$, say $\mathfrak{a} \subseteq \mathfrak{p}$ (w.l.o.g.). If now $\mathfrak{q} \in \mathbb{V}(\mathfrak{a})$ then in particular we get $\mathfrak{q} \in \mathbb{V}(\mathfrak{u})$. Thus if $\mathfrak{q} \subseteq \mathfrak{p}$ then the minimality of $\mathfrak{p}$ over $\mathfrak{u}$ implies $\mathfrak{q} = \mathfrak{p}$. That is $\mathfrak{p}$ is a minimal element of $\mathbb{V}(\mathfrak{a})$ and hence the inclusion. As both $\mathbb{V}(\mathfrak{a})_*$ and $\mathbb{V}(\mathfrak{b})_* < \infty$ are finite, $\mathbb{V}(\mathfrak{u})_* < \infty$ would have to be finite, too. But this contradicts $\mathfrak{u} \in \mathcal{A}$ again, so the assumption $\mathcal{A} \neq \emptyset$ has to be abandoned. That is any ideal $\mathfrak{a}$ of R only has finitely many prime ideals lying over it.

(ii) Consider a set of prime ideals $\mathcal{P} \neq \emptyset$ of the noetherian ring R. It has already been shown in (2.34) that $\mathcal{P}^* \neq \emptyset$ contains maximal elements. We will now prove that $\mathcal{P}_* \neq \emptyset$ contains a minimal element, as well. Suppose this was untrue, then we start with any $\mathfrak{p} = \mathfrak{p}_0 \in \mathcal{P}$. As $\mathfrak{p}_0$ is not minimal in $\mathcal{P}$, there is some $\mathfrak{p}_1$ such that $\mathfrak{p}_0 \supset \mathfrak{p}_1$. Again $\mathfrak{p}_1$ is not minimal in $\mathcal{P}$, such that we may choose some $\mathfrak{p}_2 \in \mathcal{P}$ such that $\mathfrak{p}_1 \supset \mathfrak{p}_2$. Continuing that way we find an infinite, strictly descending chain of prime ideals

$$\mathfrak{p} \;=\; \mathfrak{p}_0 \;\supset\; \mathfrak{p}_1 \;\supset\; \mathfrak{p}_2 \;\supset\; \ldots \;\supset\; \mathfrak{p}_k \;\supset\; \ldots$$

This means that $\mathfrak{p}$ is a prime ideal of infinite height $\operatorname{height}(\mathfrak{p}) = \infty$. But in a noetherian ring we have Krull's height theorem (8.80.(ii)). And this states that $\operatorname{height}(\mathfrak{p}) \leq \operatorname{rank}(\mathfrak{p}) < \infty$. Hereby the rank is finite, as any ideal $\mathfrak{p}$ in a noetherian ring is finitely generated.

□

Proof of (2.48):
We start with the equivalences for $a \mid b$. Hereby (a) $\implies$ (c) is clear: $b \in aR = \{ ah \mid h \in R \}$ yields $b = ah$ for some $h \in R$. (c) $\implies$ (b): consider $f \in bR$, that is $f = bg$ for some $g \in R$. But as $b = ah$ this yields $f = ahg \in aR$. (b) $\implies$ (a): as $b \in bR \subseteq aR$ we have $b \in aR$.
We also have to check the equivalences for $a \approx b$ - recall that now R is an integral domain. (a) $\implies$ (b): if $aR = bR$ then in particular $aR \subseteq bR$ and hence $b \mid a$. Likewise we get $a \mid b$. (b) $\implies$ (c): Suppose $b = \alpha a$ and $a = \beta b$. If $b = 0$ then $a = \beta b = \beta \cdot 0 = 0$, as well. And hence we may choose $\alpha := 1$. Thus we continue with $b \neq 0$. Then $b = \alpha a = \alpha\beta b$. And as R is an integral domain and $b \neq 0$ we may divide by b and thereby obtain $1 = \alpha\beta$. That is $\alpha \in R^*$ and $b = \alpha a$ as claimed. (c) $\implies$ (a): As $b = \alpha a$ we get $bR \subseteq aR$. And from $a = \alpha^{-1} b$ we get $aR \subseteq bR$. □

Proof of (2.51):

(i) By definition of 1 we have $1 \cdot b = b$ and hence $1 \mid b$, likewise we have $a \cdot 0 = 0$ and hence $a \mid 0$ by (1.41). Now $ah = ab$ for $h := b$ and hence $a \mid ab$ is trivial again.

(i) Next suppose $b = 0$, then $b = 0 \cdot 1$ and hence $0 \mid b$. Conversely suppose $0 \mid b$, that is there is some $h \in R$ such that $0 = 0 \cdot h = b$. Then we have just proved $0 = b$, as well. If $a \in R^*$ then $1 = aa^{-1}$ and hence $a \mid 1$. Conversely suppose $a \mid 1$, that is there is some $h \in R$ such that $ah = 1$. As R is commutative this also is $ha = 1$ and hence $a \in R^*$. Finally let $a \mid b$, that is $ah = b$ for some $h \in R$ again. In particular this yields $(ac)h = (ah)c = bc$ and hence $ac \mid bc$.

(ii) Now suppose $u \in R$ is a non-zero divisor, by (i) we only have to show the implication " $\Longleftarrow$ ". Thus let $(au)h = bu$ for some $h \in R$, then $(ah - b)u = (au)h - bu = 0$. But as u is a non-zero divisor this can only happen if $ah - b = 0$ and this already is $a \mid b$.

(iii) First of all $a \mid a$ is clear by $a \cdot 1 = a$. If now $a \mid b$ and $b \mid c$ (say $ag = b$ and $bh = c$) then we get $a \mid c$ from $a(gh) = (ag)h = bh = c$. And that $a \mid b$ and $b \mid a$ implies $a \approx b$ is true by definition (2.48).

(iv) As we have seen in (2.48) $a \approx b$ is equivalent, to $aR = bR$. And from this it is clear that $\approx$ is reflexive, symmetric and transitive (i.e. an equivalence relation). Thus it only remains to observe that

$$[a] \;=\; \{\, b \in R \mid a \approx b \,\} \;=\; \{\, \alpha a \mid \alpha \in R^* \,\} \;=\; aR^*$$

□

Proof of (2.58):

(i) The statement is clear by induction on the number k of elements involved: if $k = 1$ then $p \mid a_1$ is just the assumption. Thus consider $k+1$ elements and let $a := a_1 \ldots a_k$ and $b := a_{k+1}$. Then by assumption we have $p \mid ab$ and (as p is prime) hence $p \mid a$ or $p \mid b$. If $p \mid b$ then we are done (with $i = k+1$). And if $p \mid a$ then by induction hypothesis we find some $i \in 1 \ldots k$ such that $p \mid a_i$. Altogether $p \mid a_i$ for some $i \in 1 \ldots k+1$.

(ii) If $p \in R$ is prime then $p \neq 0$ by definition. And as also $p \notin R^*$ we have $pR \neq R$, as well. Now $ab \in pR$ translates into $p \mid ab$ and hence $p \mid a$ or $p \mid b$. But this again is $a \in pR$ or $b \in pR$. That is we have proved that pR is prime. Conversely suppose $p \neq 0$ and that pR is a prime ideal. As $pR \neq R$ we have $p \notin R^*$. And as we also assumed $p \neq 0$ this means $p \in R^\bullet$. If we are now given $a, b \in R$ with $p \mid ab$, then $ab \in pR$ and hence $a \in pR$ or $b \in pR$, as pR is prime. Thus we find $p \mid a$ or $p \mid b$ again, and altogether p is prime.

(iii) "p irreducible $\implies$ αp irreducible": suppose $\alpha p = ab$ for some $a, b \in R$. As α is a unit this yields $p = (\alpha^{-1}a)b$ and as p is irreducible hence $\alpha^{-1}a \in R^*$ or $b \in R^*$. But $\alpha^{-1}a \in R^*$ already implies $a \in R^*$ (with inverse $a^{-1} = \alpha^{-1}(\alpha^{-1}a)^{-1}$). Conversely if αp is irreducible then $p = \alpha^{-1}\alpha p$ is irreducible, too by what we have just proved.

(iii) "p prime $\implies$ αp prime": suppose $\alpha p \mid ab$ for some $a, b \in R$. As α is a unit this yields $p \mid (\alpha^{-1}a)b$ and as p is prime we hence get $p \mid \alpha^{-1}a$ or $p \mid b$. From $p \mid \alpha^{-1}a$ we get $\alpha p \mid a$ and $p \mid b$ implies $p \mid \alpha^{-1}p$ which also implies $\alpha p \mid b$. Thus we have proved, that αp is prime too. Conversely if αp is prime then $p = \alpha^{-1}\alpha p$ is prime, too by what we have just proved.

(iv) Now let R be an integral domain, $p \in R$ be prime and suppose $p = ab$ for some $a, b \in R$. In particular $p \mid ab$ and hence $p \mid a$ or $p \mid b$. W.l.o.g. let us assume $p \mid b$, that is $ph = b$ for some $h \in R$. Then we get $p = ab = aph$ and hence $p(1 - ah) = 0$. Now as $p \neq 0$ this implies $ah = 1$, that is $a \in R^*$ is a unit of R. Thereby we have verified, that p truly is irreducible.

(v) Let $f := ab$, then it is clear that $a \mid f$ and hence $fR \subseteq aR$. And as both a and $b \neq 0$ are non-zero, so is f (as R is an integral domain). Now suppose we had $a \in fR$, that is $a = fg$ for some $g \in R$. Then we compute $a = fg = abg$. And as $a \neq 0$ this means $1 = bg$. In particular $b \in R^*$ is a unit, in contradiction to $b \in R^\bullet$. Hence $a \in aR \setminus fR$ and this yields the claim $fR \subset aR$.

(vi) If $f \approx p$ then $p = \alpha f$ for some $\alpha \in R^*$ and in particular this means $f \mid p$. Conversely suppose $f \mid p$, that is there is some $a \in R$ such that $p = af$, in particular $p \mid af$. As p is prime we hence get $p \mid a$ or $p \mid f$. If $p \mid f$ then we already have $f \approx p$, as we also have $f \mid p$. So suppose we had $p \mid a$. This would mean $a = bp$ for some $b \in R$ and hence $p = af = bpf$. As R is an integral domain, we conclude $1 = bf$ such that $f \in R^*$. But as $f \notin R^*$ this is false.

(vii) As $d \mid a$ and $d \mid b$ there are some elements $\alpha = a/d$ and $\beta = b/d \in R$ such that $a = \alpha d$ and $b = \beta d$. Now consider some $\delta \in R$ such that $\delta \mid \alpha$ and $\delta \mid \beta$. That is $\alpha = u\delta$ and $\beta = v\delta$ for some u and $v \in R$. Then $a = \alpha d = u\delta d$ and $b = \beta d = v\delta d$ such that $\delta d \mid a$ and $\delta d \mid b$. Now since $d \in \gcd\{a, b\}$ is a greatest common divisor of a and b, we get $\delta d \mid d$. However it is also clear that $d \mid \delta d$ which implies $d \approx \delta d$. Now as R is an integral domain this yields $\delta \in R^*$. But as $\delta \in R$ only needed to satisfy $\delta \mid \alpha$ and $\delta \mid \beta$ this means $1 \in \gcd\{\alpha, \beta\}$.

(viii) Clearly we have $R^* \subseteq D$, as $k = 0$ is allowed. And if $c = \alpha p_1 \dots p_k$ and $d = \beta q_1 \dots q_l \in D$ it is clear that $cd = (\alpha\beta)(p_1 \dots p_k q_1 \dots q_l) \in D$ again. Thus it remains to show the implication $cd \in D$ $\implies$ $c \in D$ (due to the symmetry of the statement it also follows that $d \in D$). Thus consider any $c, d \in R$ such that $cd = \alpha p_1 \dots p_k \in D$. We will prove the claim by induction on k - that is we will verify

$$\forall\, c, d \in R \,:\, cd = \alpha p_1 \dots p_k \in D \quad \implies \quad c \in D$$

for any $k \in \mathbb{N}$. The case $k = 0$ is trivial, since $cd = \alpha \in R^*$ implies $c \in R^* \subseteq D$. Thus regard $k \geq 1$. We let $I := \{i \in 1 \dots k \mid p_i \mid d\}$. (1) If there is some $i \in I$ then $p_i \mid b$. W.l.o.g. we may assume $i = k$. That is there is some $h \in R$ such that $d = hp_k$. Then

$$\alpha p_1 \dots p_k \;=\; cd \;=\; chp_k$$

As R is an integral domain and $p_k \neq 0$ we may divide by p_k to find $ch = \alpha p_1 \dots p_{k-1} \in D$. By induction hypothesis that is $c \in D$ already. (2) If $I = \emptyset$ then for any $i \in 1 \dots k$ we've got $p_i \nmid d$. But as p_k is prime and $p_k \mid cd$ this yields $p_k \mid c$, say $c = gp_k$. Then

$$\alpha p_1 \dots p_k \;=\; cd \;=\; gdp_k$$

We divide by p_k again to find $gd = \alpha p_1 \dots p_{k-1} \in D$. And by induction hypothesis this means $g \in D$. But $p_k \in D$ is clear, as well and therefore $c = gp_k \in D$ as claimed.

(ix) First consider the case $\alpha = 1 = \beta$. Without loss of generality we may assume $k \leq l$ and we will use induction k to prove the statement. If $k = 0$ we have to prove $l = 0$. Thus assume $l \geq 1$ then $1 = q_1 \dots q_l = q_1(q_2 \dots q_l)$. That is $q_1 \in R^*$ is a unit. But q_1 has been prime and hence $q_1 \notin R^*$ a contradiction. Thus we necessarily have $k = l = 0$. Now consider the induction step $k \geq 1$, then $p_k \mid p_1 \dots p_k = q_1 \dots q_l$ and as p_k is prime this means $p_k \mid q_j$ for some $j \in 1 \dots l$. Without loss of generality we may assume $j = l$. Hence we found $q_l = \gamma p_k$ for some $\gamma \in R$. But q_l has been prime and hence is irreducible by (iv). This means $\gamma \in R^*$ (as $p_k \notin R^*$) and hence $p_k \approx q_k$. Further we have

$$(p_1 \dots p_{k-1})p_k \;=\; p_1 \dots p_k \;=\; q_1 \dots q_l \;=\; \gamma(q_1 \dots q_{l-1})p_k$$

As $p_k \neq 0$ and R is an integral domain we may divide by p_k and thereby get $p_1 \dots p_{k-1} = (\gamma q_1)q_2 \dots q_{l-1}$. (As γq_1 is prime again) the induction hypothesis now yields that $k - 1 = l - 1$ and there is some $\sigma \in S_{k-1}$ such that for any $i \in 1 \dots k-1$ we have $p_i \approx q_{\sigma(i)}$. But this also is $k = l$ and we may extend σ to S_k by letting $\sigma(k) := k = l$. (As $q_1 \approx \gamma q_1$) we hence found $p_i \approx q_{\sigma(i)}$ for any $i \in 1 \dots k$. Thus we have completed the case $\alpha = 1 = \beta$. If now α and $\beta \in R^*$ are arbitrary, then we let $p'_1 := \alpha p_1$, $p'_i := p_i$ (for $i \in 2 \dots k$) and $q'_1 := \beta q_1$, $q'_j := q_j$ (for $j \in 2 \dots l$). By (iii) p'_i and q'_j are prime again and by construciton it is clear that $p'_i \approx p_i$ and $q'_j \approx q_j$ for any $i \in 1 \dots k$ and $j \in 1 \dots l$. As $p'_1 \dots p'_k = q'_1 \dots q'_l$ we may invoke the first case to find $k = l$ and the required permutation $\sigma \in S_k$. But now for any $i \in 1 \dots k$ we get $p_i \approx p'_1 \approx q'_{\sigma(i)} \approx q_{\sigma(i)}$ and hence $p_i \approx q_{\sigma(i)}$ as claimed.

(x) We only prove the equivalence for the least common multiple (the like statement for the greatest common divisor can be proved in complete analogy). Clearly $m \in mR^* = \operatorname{lcm}(A)$ implies $m \in \operatorname{lcm}(A)$. Thus let us assume $m \in \operatorname{lcm}(A)$, then we need to prove $\operatorname{lcm}(A) = mR^*$. For " $\supseteq$ " we are given any $\alpha \in R^*$. As $A \mid m$ it is clear that $A \mid \alpha m$, as well. And if $A \mid n$ then $m \mid n$ (by assumption) and hence also $\alpha m \mid n$ (by $(\alpha m)(\alpha^{-1}h) = n$ for $mh = n$). Concersely for " $\subseteq$ " consider $n \in \operatorname{lcm}(A)$. As $A \mid m$ and $n \in \operatorname{lcm}(A)$ we get $n \mid m$. Analogously $A \mid n$ and $m \in \operatorname{lcm}(A)$ impliy $m \mid n$. Together that is $m \approx n$ and hence $n = \alpha n$ for some $\alpha \in R^*$.

□

Proof of (2.57):

(i) If $A = \{a\}$ then $A \mid a$ is clear. Also $A \mid n$ is $a \mid n$ [for any $n \in R$] such that $A \mid n$ trivially implies $a \mid n$. Therefore $a \in \operatorname{lcm}(A)$. And $a \in \gcd(A)$ can be seen in complete analogy.

(ii) Let us denote $B := A \cup \{1\}$, then $B \mid n$ is equivalent to $A \mid n$ [for any $n \in R$], as $1 \mid n$ is always satisfied. In particular properties (1) of a least common multiple $m \in R$ of A and B are the same. Linekwise for property (2) $B \mid n \implies m \mid n$. As we can substitute $B \mid n$ by $A \mid n$ property (2) agrees, as well. From this we find that $m \in \operatorname{lcm}(B)$ is equivalent to $m \in \operatorname{lcm}(A)$.

Likewise for $B := A \cup \{0\}$ we find that $c \mid B$ is equivalent to $c \mid A$ [for any $c \in R$], as $c \mid 0$ is always satisfied. In complete analogy to the above we find that $d \in \gcd(B)$ is equivalent to $d \in \gcd(A)$.

(iii) If $A = \{0\}$ then we have already seen $0 \in \gcd(A)$ and $0 \in \operatorname{lcm}(A)$ in (i). It remains to show the converse implications: If $0 \in \gcd(A)$ then in particular $0 \mid A$. That is for any $a \in A$ we have $0 \mid a$. But this means $a = 0$ such that necessarily $A = \{0\}$.

Now let R be an integral domain and A be finite. Suppose we had $A \neq \{0\}$, letting $A' := A \setminus \{0\} \neq \emptyset$ (ii) tells us that $\operatorname{lcm}(A) = \operatorname{lcm}(A')$. As A is finite, so is A' say $A' = \{a_1, \ldots, a_k\}$. By assumption we have $0 \in \operatorname{lcm}(A) = \operatorname{lcm}(A')$ and in particular this means $A \mid n \implies n = 0$ for any $n \in R$. Therefore for any $n \neq 0$ we necessarily have $A \nmid n$, that is there is some $a \in A$ such that $a \nmid n$. Now take $n := a_1 \ldots a_k$ as R is an integral domain and $a_i \neq 0$ we also have $n \neq 0$. By assumption there is some $a_i \in A'$ such that $a_i \nmid n = a_1 \ldots a_k$ which is absurd. This contradicion yields $A' = \emptyset$ and hence $A = \{0\}$.

(iv) We only need to prove $\mathbb{N} \mid k \iff k = 0$ for any $k \in \mathbb{Z}$. If $k = 0$ then $k = 0 = n \cdot 0$ for any $n \in \mathbb{N}$ and hence $n \mid k$. Conversely suppose $\mathbb{N} \mid k$, then we choose $n := 2|k| \in \mathbb{N}$. As $n \mid k$ there is some $a \in \mathbb{Z}$ such that $\pm 2ak = an = k$ or equivalently $k(1 \mp 2a) = 0$. As 2 is not a unit of $\mathbb{Z}$ this only leaves $k = 0$. And form this equivalence it is clear, that $\operatorname{lcm}(\mathbb{Z}) = \{0\}$.

□

Proof of (2.59):

(i) Suppose $\langle a \mid b \rangle = \infty$ that is for any $k \in \mathbb{N}$ there is some $h_k \in R$ such that $a^k h_k = b$. First suppose there was some $k \in \mathbb{N}$ such that $h_k = 0$. Then $b = a^k \cdot 0 = 0$, too and then $a \mid 0$ also implies $a = 0$, a contradiction. Thus $h_k \neq 0$ for any $k \in \mathbb{N}$. Now for any $k \in \mathbb{N}$ we find $h_{k+1} a^{k+1} = b = h_k a^k$. And as $a \neq 0$ and R is an integral domain $h_{k+1} a^{k+1} = h_k a^k$ also yields $h_{k+1} a = h_k$. That is $h_{k+1} \mid h_k$ and hence we have found the ascending chain of ideals

$$h_0 R \subseteq h_1 R \subseteq \ldots \subseteq h_k R \subseteq h_{k+1} R \subseteq \ldots$$

Now suppose we had $h_k R = h_{k+1} R$ at any one stage $k \in \mathbb{N}$. That is there is some $\alpha \in R$ such that $h_{k+1} = \alpha h_k$. Thereby we compute $h_k = a h_{k+1} = \alpha a h_k$. And as $h_k \neq 0$ this implies $\alpha a = 1$. That is $a \in R^*$ a contradiction to $a \in R^\bullet$. And this only leaves $\langle a \mid b \rangle < \infty$.

(ii) As p is prime we have $p \in R^\bullet$ and hence $\langle p \mid a \rangle < \infty$ due to (i) (likewise for b and ab). That is we let $k := \langle p \mid a \rangle$, $l := \langle p \mid b \rangle$ and $n := \langle p \mid ab \rangle \in \mathbb{N}$. Then by assumption there are some α, $\beta \in R$ such that $a = \alpha p^k$ and $b = \beta p^l$. In particular $ab = \alpha\beta p^{k+1}$ such that $p^{k+l} \mid ab$ and

hence $k+l \leq n$, as n is maximal among the integers with $p^n \mid ab$. Now suppose $n > k+l$, say $p^n h = ab = \alpha\beta p^{k+l}$. As R is an integral domain we may divide by p^{k+l} and thereby obtain $p^{n-(k+l)}h = \alpha\beta$. And as $n-(k+l) \geq 1$ this yields $p \mid \alpha\beta$. Now recall that p has been prime, then we may assume (w.l.o.g.) that $p \mid \alpha$, say $pg = \alpha$. Then $a = \alpha p^k = gp^{k+1}$ and hence $p^{k+1} \mid a$. But this is a contradiction to k being maximal and hence the assumption $n > k+l$ has to be dropped. Altogether we have found $n = k+l$.

The second property is an immediate consequence of the first: If $n = 0$, then $a^n = 1$ and $p \not| 1$, as p is a non-unit. We now use induction on n, $\langle p \mid a^{n+1}\rangle = \langle p \mid a\rangle + \langle p \mid a^n\rangle$ by the above. But by induction hypothesis, this is $\langle p \mid a\rangle + n \cdot \langle p \mid a\rangle = (n+1) \cdot \langle p \mid a\rangle$.

(♡) In a first step let us prove, that for any $a \in R^\bullet$ there is an irreducible $p \in R$ such that $p \mid a$. To do this we recursively define a sequence of elements, starting with $a_0 := a$. Now suppose we had already constructed $a_0, \ldots, a_k \in R$ such that $a_0R \subset a_1R \subset \ldots \subset a_kR$. Of course $a_k = 0$ cannot be, as $0 \neq a = a_0 \in a_kR$. Then we iterate as follows: if a_k is not irreducible then there are f, $g \in R^\bullet$ such that $a_k = fg$. Then by (2.58.(iv)) we get $a_kR = (fg)R \subset fR$. Thus if we now let $a_{k+1} := f$ then we have appended our chain of ideals to

$$a_0R \subset a_1R \subset \ldots \subset a_kR \subset a_{k+1}R$$

As R is noetherian we cannot construct a strictly ascending chain of infinite length. That is our construction has to terminate at some finite level $s \in \mathbb{N}$. And this can only be if $p := a_s$ is irreducible. Thus we have $a = a_0 \in a_0R \subseteq a_sR = pR$ and thereby $p \mid a$.

(iii) If $a \in R^*$ is a unit, then the claim is clear by choosing $\alpha := a$ and $k := 0$. Thus let us assume $a \in R^\bullet$. Then by (♡) above there is some irreducible element $p_1 \in R$ such that $p_1 \mid a$, say $p_1a_1 = a$. Thus suppose we have already constructed the elements $a_1, \ldots, a_k \in R$ and $p_1, \ldots, p_k \in R$ such that the p_i are irreducible, $a = a_kp_1 \ldots p_k$ and $aR \subset a_1R \subset \ldots \subset a_kR$. Suppose that $a_k \notin R^*$ is no unit, then we iterate as follows: Note that $a_k \neq 0$ as well (else $a = 0$) and hence $a_k \in R^\bullet$. Thus by (♡) there is some irreducible element $p_{k+1} \in R$ such that $p_{k+1} \mid a_k$, say $a_k = p_{k+1}a_{k+1}$. We note that by (2.58.(iv)) this implies $a_kR = (p_{k+1}a_{k+1})R \subset a_{k+1}R$. So we have found a_{k+1} and p_{k+1} irreducible such that $a_{k+1}p_1 \ldots p_{k+1} = a_kp_1 \ldots p_k = a$ and

$$aR \subset a_1R \subset \ldots \subset a_kR \subset a_{k+1}R$$

As R is noetherian we cannot construct a strictly ascending chain of infinite length. That is our construction has to terminate at some finite level $s \in \mathbb{N}$. And this can only be if $a_s \in R^*$ is a unit. Thus we let $\alpha := a_s$ and thereby get $a = \alpha p_1 \ldots p_s$ as claimed.

(iv) As R is noetherian and $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ is an ideal there are finitely many $a_i \in R$ such that $\mathfrak{p} = \langle a_1, \ldots, a_k\rangle_{\mathrm{i}}$. Without loss of generality we may assume $a_i \neq 0$ (else we might just as well drop it). Then we use (iii) to find a decomposition of a_i into irreducible elements $p_{i,j} \in R$

$$a_i = \alpha_i \prod_{j=1}^{n(i)} p_{i,j}$$

As $a_i \in \mathfrak{p}$ and $\mathfrak{p}$ is prime this means that for any $i \in 1 \ldots k$ there is some $j(i) \in 1 \ldots n(i)$ such that $p_{i,j} \in \mathfrak{p}$ (note that $\alpha_i \neq \mathfrak{p}$ as else $1 = \alpha_i^{-1}\alpha_i \in \mathfrak{p}$). Now let $p_i := p_{i,j(i)} \in \mathfrak{p}$. Then it is clear that

$$a_i \in p_i R \subseteq \langle p_1, \ldots, p_k \rangle_{\mathfrak{i}} \subseteq \mathfrak{p} = \langle a_1, \ldots, a_k \rangle_{\mathfrak{i}}$$

for any $i \in \ldots k$. And thereby $\mathfrak{p} = \langle a_1, \ldots, a_k \rangle_{\mathfrak{i}} \subseteq \langle p_1, \ldots, p_k \rangle_{\mathfrak{i}}$ as well such that we truly find $\mathfrak{p} = \langle p_1, \ldots, p_k \rangle_{\mathfrak{i}}$ as claimed.

(vi) Let us prove the first statement $a \mid b$ by induction over k. If $k = 0$ then $a = 1$ and hence $a \mid b$ is clear. Let us now fix some some abbreviations: let $n(i) := \langle q_i \mid b \rangle \in \mathbb{N}$ due to (i). And by definition of $\langle q_i \mid b \rangle$ it is clear that $q_i^{n(i)} \mid b$, say $b = b_i q_i^{n(i)}$ for any $i \in 1 \ldots k$. Hence in case $k = 1$ we are done already, as $a = q_1^{n(1)} \mid b$. Thus we may assume $k \geq 2$. Then the induction hypothesis reads as

$$h := \prod_{i=1}^{k-1} q_i^{n(i)} \;\Big|\; b$$

Assume that $q_k \mid h$, as q_k is prime (by construction of h) this would mean $q_k \mid q_i$ for some $i \in 1 \ldots k-1$. That is $q_i = \alpha_i q_k$ for some $\alpha_i \in R$. But as R is an integral domain and q_i is prime it also is irreducible by (2.58.(v)). This yields $\alpha_i \in R^*$ and hence $q_i \approx q_k$. But by assumption this is $i = k$ in contradiction to $i \in 1 \ldots k-1$. Thus we have seen $q_k \not| h$, or in other words $\langle q_k \mid h \rangle = 0$. Now recall that $h \mid b$, that is there is some $g \in R$ such that $b = gh$. then we may easily compute (using (ii))

$$n(k) = \langle q_k \mid b \rangle = \langle q_k \mid gh \rangle = \langle q_k \mid g \rangle + \langle q_k \mid h \rangle = \langle q_k \mid g \rangle$$

That is $q_k^{n(k)} = q_k^{\langle q_k | g \rangle} \mid g$ such that $g = q_k^{n(k)} f$ for some $f \in R$. Multiplying this identity with h we finally find $a \mid b$ from

$$b = gh = q_k^{n(k)} fh = af$$

It remains to verify the second claim in (vi). That is consider any prime element $p \in R$ such that $p \mid b = af$. As p is prime this means $p \mid a$ or $p \mid f$. In the first case $p \mid a$ (by construction of a) we find some $i \in 1 \ldots k$ such that $p \mid q_i$. That is $\alpha p = q_i$ for some $\alpha \in R$. Again we use that q_i is prime and hence irreducible to deduce that $\alpha \in R^*$ and hence $p \approx q_i$. In the second case $p \mid f$ we are done already, as $f = b/a$. Thus we have proved $p \mid (b/a)$ *or* $p \approx p_i$ for some $i \in 1 \ldots k$. Now suppose *both* statements would be true, that is $p \mid f$ *and* (w.l.o.g.) $p \mid q_k$. That is $f = pr$ and $q_k = \alpha p$ for some $r \in R$ and $\alpha \in R^*$. Then we compute

$$b = af = \big(hq_k^{n(k)}\big)\big(\alpha^{-1} q_k r\big) = q_k^{n(k)+1}\big(\alpha^{-1} hr\big)$$

In particular $q_k^{n(k)+1} \mid b$. But this clearly is a contradiction to the maximality of $n(k) = \langle q_k \mid b \rangle$. Thus we have proved the truth of *either* $p \mid (b/a)$ *or* $p \approx q_i$ (and not *both*) as claimed.

(v) Suppose we had $a \in pR$ for infinitely many $p \in P$. In particular we may choose a countable subset $(p_i) \subseteq P$ such that $a \in p_i R$ for any $i \in \mathbb{N}$. By (vi) we get

$$a_k := \prod_{i=0}^{k} p_i^{\langle p_i | a \rangle} \;\Big|\; a$$

From the construction it is clear that for $f_k := p_k^{\langle p_k | a \rangle}$ we get $a_{k-1} f_k = a_k$. And as $p_k \mid a$ we have $\langle p_k \mid a \rangle \geq 1$ such that $f_k \neq 1$. In fact $f_k \in R^\bullet$ as $p_k \in R^\bullet$ and R is an integral domain. Next let us choose some $g_k \in R$ such that $a = a_k g_k$. Then for any $k \in \mathbb{N}$ we get $a_k g_k = a = a_{k+1} g_{k+1} = a_k f_{k+1} g_{k+1}$. It is clear that $a_k \neq 0$, as else $a = 0 \cdot g_k = 0$. Thus we may divide a_k from $a_k g_k = a_k f_{k+1} g_{k+1}$ and thereby find $g_k = f_{k+1} g_{k+1}$. Now using (2.58.(iv)) with $g_{k+1} \neq 0$ and $f_{k+1} \in R^\bullet$ we find $g_k R \subset g_{k+1} R$. As this is true for any $k \in \mathbb{N}$ we have found an infinitely ascending chain

$$g_0 R \subset g_1 R \subset g_2 R \subset \dots$$

of ideals in R. But this is a contradiction to R being noetherian. Thus the assumption has to be false and that is: there are only finitely many $p \in P$ with $a \in pR$.

□

Proof of (2.60):

In a first step we will prove the equivalence of (a), (b) and (c). Using these as a definition we will prove some more properties of UFDs first, before we continue with the proof of the equivalences of (d), (e) and (f) on page (1100).

- (a) $\implies$ (c): By (2.58.(v)) we already know that prime elements are irreducible (as R is an integral domain). From this (1) and the one part of (2) are trivial by assumption (a). We only have to prove the second part of (2): $\forall\, q \in R : q$ irreducible $\implies q$ prime. By assumption (a) q admits a prime decomposition $q = \alpha p_1 \dots p_k$. It is clear that $k \neq 0$ as else $q \in R^*$. Now suppose $k \geq 2$ then we would write q as $q = (\alpha q_1)(q_2 \dots q_k)$. And as q is irreducible this would mean $\alpha p_i \in R^*$ or $p_2 \dots p_k \in R^*$. But as p_1 is prime, so is αp_1 - by (2.58.(iii)) - and as R is an integral domain $R^\bullet$ is closed under multiplication such that $p_2 \dots p_k \in R^\bullet$. Hence none of this can be and this only leaves $k = 1$. That is $q = \alpha p_1$ and hence q is prime.

- (c) $\implies$ (b): consider any $0 \neq a \in R$, property (1) in (b) and (c) are identical so we only need to verify (2) in (b). Thus let $(\alpha, p_1, \dots, p_k)$ and $(\beta, q_1, \dots, q_l)$ be two irreducible decompositions of a. By assumption (2) in (c) all the p_i and p_j are prime already. Therefore $\alpha p_1 \dots p_k = a = \beta q_1 \dots q_l$ implies $k = l$ and $p_i = q_{\sigma(i)}$ (for some $\sigma \in S_k$ and any $i \in 1 \dots k$) by (2.58.(vii)). And by definition this already is $(\alpha, p_1, \dots, p_k) \approx (\beta, q_1, \dots, q_l)$.

- (b) $\implies$ (a): By assumption (b) any $0 \neq a \in R$ has an irreducible decomposition. Thus it suffices to show that any irreducible element $p \in R$ already is prime. Thus consider an irreducible $p \in R$ and arbitrary $a, b \in R$. Then we need to show $p \mid ab \implies p \mid a$ or $p \mid b$. To do this we write down irreducible decompositions of a and b

$$a = \alpha p_1 \dots p_k \quad \text{and} \quad b = \beta p_{k+1} \dots p_{k+l}$$

As $p \mid ab$ there is some $h \in R$ with $ab = ph$. Again we use an irreducible decomposition of $h = \gamma q_1 \dots q_m$. Finally let $q_{m+1} := p$

$$\gamma q_1 \dots q_m q_{m+1} = ph = ab = \alpha\beta p_1 \dots p_{k+l}$$

As all the p_i and q_j are irreducible assumption (2) now yields that $n := m + 1 = k + l$ and that

there is some $\sigma \in S_n$ such that for any $i \in 1 \ldots n$ we get $q_i \approx p_{\sigma(i)}$. Now let $j := \sigma(m+1)$, that is $p = q_{m+1} \approx p_j$. If $j \in 1 \ldots k$ then $p \approx p_j \mid a$ and hence $p \mid a$. Likewise if $j \in k+1 \ldots k+l$ then $p \approx p_j \mid b$ and hence $p \mid b$. Together this means that p is truly prime.

□

Proof of (2.64):
Until now we only have proved the equivalence of (a), (b) and (c) in the definition of an UFD. That is we understand by an UFD an integral domain satisfying (a) (equivalently (b) or (c)). And using this definition only we are able to prove the theorem given:

(i) Let $I := \{i \in 1 \ldots k \mid p \approx p_i\}$ and $n := \#I$. Then for any $i \in I$ there is some $\alpha_i \in R^*$ such that $p_i = \alpha_i p$. Then it is immediately clear that

$$a \;=\; \beta b p^n \quad \text{where} \quad \beta := \alpha \prod_{i \in I} \alpha_i \quad \text{and} \quad b := \prod_{j \notin I} p_j$$

In particular $p^n \mid a$ and this means $n \leq \langle p \mid a \rangle$. Conversely suppose $p^m \mid a$ for some $m > n$, say $p^m h = a = \beta b p^n$. Then $p^{m-n} \beta^{-1} h = b$ and hence $p \mid b$ as $p \mathrm{dim} p^{m-n}$. By definition of b this would imply $p \mid p_j$ for some $j \notin I$. Say $p_j = \gamma p$ for some $\gamma \in R$. But as p_j is irreducible (and $p \notin R^*$ this yields $\gamma \in R^*$ and hence $p \approx p_j$ in contradiction to $j \notin I$. Thus we have proved the maximality of n and hence $n = \langle p \mid a \rangle$.

(ii) Using (i) this boils down to an easy computation: pick up two prime decompositions $a = \alpha p_1 \ldots p_k$ and $b = \beta q_1 \ldots q_l$. For $j \in 1 \ldots l$ we let $p_{k+j} := q_j$. Then it is clear that $ab = \alpha\beta p_1 \ldots p_{k+l}$ and thereby

$$\begin{aligned} \langle p \mid ab \rangle &= \#\{\, i \in 1 \ldots (k+l) \mid p \approx p_i \,\} \\ &= \#\{\, i \in 1 \ldots k \mid p \approx p_i \,\} + \#\{\, j \in 1 \ldots l \mid p \approx q_j \,\} \\ &= \langle p \mid a \rangle + \langle p \mid b \rangle \end{aligned}$$

The reasoning for the power to multiple property is precisely the same, as in the case of a noetherian integral domain, please refer to (2.59.(ii)).

(v) *Existence:* consider any $0 \neq a \in R$ and pick up a prime decomposition $a = \beta q_1 \ldots q_k$ of a. As the q_i is prime there is a uniquely determined $p_i \in \mathbb{P}$ such that $q_i \approx p_i$, say $q_i = \alpha_i p_i$ for some $\alpha_i \in R^*$. Then

$$a = \alpha p_1 \ldots p_k \quad \text{where} \quad \alpha := \alpha_1 \ldots \alpha_k$$

For any $p \in \mathbb{P}$ now let $n(p) := \#\{\, i \in 1 \ldots k \mid p_i = p \,\} \in \mathbb{N}$. Then it is clear that only finitely many $n(p)$ are non-zero, as they sum up to

$$\sum_{p \in \mathbb{P}} n(p) \;=\; k$$

That is $n \in \oplus_p \mathbb{N}$ And further it is clear that a has the representation

$$a \;=\; \alpha \prod_{i=1}^{k} p_i \;=\; \alpha \prod_{p \in \mathbb{P}} p^{n(p)}$$

Uniqueness: Consider any $a \neq 0$ represented as $a = \alpha \prod_p p^{n(p)}$ as presented in the theorem. Then we fix any $q \in \mathbb{P}$, it is clear that

$$a \;=\; \alpha h q^{n(q)} \quad \text{where} \quad h := \prod_{p \neq q} p^{n(p)}$$

It is clear that $\langle q \mid q^n \rangle = n$, as $q^n \mid q^n$ and $q^{n+1} \mid q$ would imply $q \mid 1$ and hence $q \in R^*$. Further it is easy to see that $\langle q \mid \alpha h \rangle = 0$. Because if $q \mid \alpha h$ then $q \mid h$ (as $\alpha \in R^*$) and hence there has to be some $p \neq q$ such that $q \mid p$. That would be $q \approx p$ due to the irreducibility of p in contradiction to $p \neq q$ (as $\mathbb{P}$ was a representing system). Hence we may use (i) again to find

$$\langle q \mid a \rangle \;=\; \langle q \mid \alpha h q^{n(q)} \rangle \;=\; \langle q \mid \alpha h \rangle + \langle q \mid q^{n(q)} \rangle \;=\; n(q)$$

In particular the exponent $n(q)$ in this representation of a is uniquely determined to be $\langle q \mid a \rangle$. And as q has been arbitrary this means that n is uniquely determined. And as R is an integral domain this finally yields that α is uniquely determined, as well.

(iii) Suppose $b = ah$ for some $h \in R$. Then for any $p \in R$ prime we get $\langle p \mid b \rangle = \langle p \mid ah \rangle = \langle p \mid a \rangle + \langle p \mid h \rangle \geq \langle p \mid a \rangle$. Conversely suppose $\langle p \mid a \rangle \leq \langle p \mid b \rangle$ for any $p \in R$ prime. Pick up a representing system $\mathbb{P}$ and use it to write a and b in the form

$$a \;=\; \alpha \prod_{p \in \mathbb{P}} p^{m(p)} \quad \text{and} \quad b \;=\; \beta \prod_{p \in \mathbb{P}} p^{n(p)}$$

By assumption we have $m(p) = \langle p \mid a \rangle \leq \langle p \mid b \rangle = n(p)$. That is $k(p) := n(p) - m(p) \geq 0$. Hence we explicitly find some $h \in R$ such that

$$b \;=\; ah \quad \text{where} \quad h \;:=\; \alpha^{-1} \beta \prod_{p \in \mathbb{P}} p^{k(p)}$$

(iv) Pick up a representing system $\mathbb{P} \subseteq R^\bullet$ of the prime elements of R modulo associateness. Then according to (v) we find

$$\begin{aligned} a &= \alpha \prod_{p \in \mathbb{P}} p^{\langle p|a \rangle} \\ b &= \beta \prod_{p \in \mathbb{P}} p^{\langle p|b \rangle} \end{aligned}$$

for some units $\alpha, \beta \in R^*$. Hence $ab = \alpha\beta \prod_p p^{\langle p|a\rangle + \langle p|b\rangle}$ such that (iii) applied to $d \mid ab$ yields the following upper bound

$$\forall\, p \in \mathbb{P} \;:\; \langle p \mid d \rangle \;\leq\; \langle p \mid a \rangle + \langle p \mid b \rangle$$

If there was some $p \in \mathbb{P}$ with $\langle p \mid a \rangle \neq 0$ and $\langle p \mid d \rangle \neq 0$ then p would be a common divisor of a and d in contradiction to $1 \in \gcd\{a, d\}$. Hence we have

$$\forall\, p \in \mathbb{P} \;:\; \langle p \mid d \rangle \neq 0 \implies \langle p \mid a \rangle = 0$$

That is we get $\langle p \mid d \rangle \leq \langle p \mid b \rangle$ for any $p \in \mathbb{P}$ with $\langle p \mid d \rangle \neq 0$. In case $\langle p \mid d \rangle = 0$ however

$\langle p \mid d\rangle \leq \langle p \mid b\rangle$ is satisfied trivially. So we altogether have $\langle p \mid d\rangle \leq \langle p \mid b\rangle$ for *any* $p \in \mathbb{P}$. And according to (iii) again, this truly implies $d \mid b$.

(vi) Let us abbreviate $d := \prod_p p^{m(p)}$ then we need to verify that d is a greatest common divisor of A. By definition of $m(p)$ we have $\langle p \mid d\rangle = m(p) \leq \langle p \mid a\rangle$ for any $p \in \mathbb{P}$ and any $a \in A$. And by (iii) that is $d \mid a$ and for any $a \in A$ and hence $d \mid A$. Conversely consider any $c \in R$ with $c \mid A$. In particular we have $c \neq 0$ as $0 \notin A \neq \emptyset$. And hence $c \mid a$ implies $\langle p \mid c\rangle \leq \langle p \mid a\rangle$ for any $p \in \mathbb{P}$ (and $a \in A$) by (iii) again. This is $\langle p \mid c\rangle \leq m(p) = \langle p \mid d\rangle$ for any $p \in \mathbb{P}$ and hence $c \mid d$ by (iii). The statement for the least common multiple can be proved in complete analogy. We only have to note that the assumption $\#A < \infty$ guarantees $n \in \oplus_p \mathbb{N}$ again.

(vii) Once more we choose a representing system $\mathbb{P}$ of the primes of R. And for any $p \in \mathbb{P}$ let us abbreviate $m(p) := \min\{\langle p \mid a\rangle, \langle p \mid b\rangle\}$ and likewise $n(p) := \min\{\langle p \mid a\rangle, \langle p \mid b\rangle\}$. Then it is a standard fact that $m(p) + n(p) = \langle p \mid a\rangle + \langle p \mid b\rangle$. By (ii) and (v) that is

$$\begin{aligned} \langle p \mid ab\rangle &= \langle p \mid a\rangle + \langle p \mid b\rangle = m(p) + n(p) \\ &= \langle p \mid a\rangle + \langle p \mid b\rangle = \langle p \mid dm\rangle \end{aligned}$$

And as this holds true for any $p \in \mathbb{P}$ (iv) immediately yields the claim.

(viii) We commence with the notation of (vi) and choose any $e \in \gcd\{a, b, c\}$. Then by (v) the order of $p \in \mathbb{P}$ in c is given to be the following

$$\begin{aligned} \langle p \mid e\rangle &= \min\{\, \langle p \mid a\rangle, \langle p \mid b\rangle, \langle p \mid c\rangle \,\} \\ &= \min\{\, \min\{\, \langle p \mid a\rangle, \langle p \mid b\rangle \,\}, \langle p \mid c\rangle \,\} \\ &= \min\{\, \langle p \mid d\rangle, \langle p \mid c\rangle \,\} = \langle p \mid e'\rangle \end{aligned}$$

And the latter is the order of any greatest common divisor of $e' \in \gcd\{c, d\}$. As this is true for any $p \in \mathbb{P}$ we thereby find that e and e' are associated. The claim for the greatest common divisors follows immediately. The analogous argumentation also rests the case for the least common multiples.

□

Proof of (2.65):
As R is an UFD, it is an integral domain, by definition. Thus choose any $0 \neq x = b/a \in \mathrm{QUOT}(R)$ that is integral over R, i.e. $\exists\, a_1, \ldots, a_n \in R$ with

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

Then we need to show that $a \mid b$ already. But as R is an UFD we may let $d := \gcd\{a, b\}$ and write $a = \alpha d$ and $b = \beta d$. Then α and β are relatively prime and $a \mid b$ can be put as $\alpha \in R^*$ (as then $b = (\alpha^{-1}\beta)a$). By multiplying the above equation with α^n we find (note $x = \beta/\alpha$)

$$\beta^n + \alpha\,(a_1\beta^{n-1} + \cdots + \alpha^{n-1}a_n) = 0$$

And hence α divides β^n - but as α and β were relatively prime, so are α and β^n. But together this implies that α truly is a unit of R. □

Proof of (2.66):

(ii) We first prove the irreducibility of $2 \in \mathbb{Z}[\sqrt{-3}]$. Thus let $\omega := i\sqrt{3}$ and suppose $2 = (a+b\omega)(c+d\omega)$. Then by complex conjugation we find $2 = (a-b\omega)(c-d\omega)$. Multiplying these two equations we get

$$4 \;=\; 2\cdot 2 \;=\; (a^2+3b^2)(c^2+3d^2) \;\geq\; 9(bd)^2$$

Thus if both $b \neq 0$ and $d \neq 0$ this formula ends up with the contradicion $4 \geq 9(bd)^2 \geq 9$. Thus without loss of generality (interchanging a, c and b, d if necessary) we may assume $d = 0$. Then we have

$$4 \;=\; (a^2+3b^2)c^2$$

Of course $c = 0$ cannot be (else $4 = 0$). If $|c| = 1$ then $c + d\omega = \pm 1$ which of course is a unit in $\mathbb{Z}[\sqrt{-3}]$. Thus suppose $|c| \geq 2$ then $c^2 \geq 4$ such that necessarily $a^2 + 3b^2 = 1$. This of course can only be if $a = 1$ and $b = 0$ such that now $a + b\omega$ is a unit of $\mathbb{Z}[\sqrt{-3}]$. Altogether 2 is irreducible.

- On the other hand $2 \mid 4 = (1+\omega)(1-\omega)$. Now suppose we had $2 \mid 1+\omega$, say $2(a+b\omega) = 1+\omega$. Then $2a = 1$ and hence $2 =\in \mathbb{Z}^*$ which is false. Likewise we see that 2 does not divide $1-\omega$ and this means that 2 is not prime.

(iii) We first prove that $p = s^2 + t^2 - 1$ is irreducible in $\mathbb{R}[s,t]$. To do this we fix the graded lexicographic order on $\mathbb{R}[s,t]$, that is $\mathbb{R}[s,t]$ is ordered by (total) degree and by $s < t$. Now consider any two polynomials $f, g \in \mathbb{R}[s,t]$ such that $fg = p$. Then

$$\mathrm{lt}(f)\mathrm{lt}(g) \;=\; \mathrm{lt}(fg) \;=\; \mathrm{lt}(p) \;=\; \mathrm{lt}(-1+s^2+t^2) \;=\; t^2$$

By prime decomposition of the leading coefficient in $\mathbb{R}[s,t]$ we see that either $lt(f) = 1$, $\mathrm{lt}(f) = t$ or $\mathrm{lt}(f) = t^2$. If $\mathrm{lt}(f) = 1$ then f is a unit in $\mathbb{R}[s,t]$, likewise if $\mathrm{lt}(f) = t^2$ then $\mathrm{lt}(g) = 1$ and hence g is a unit in $\mathbb{R}[s,t]$. thus we only have to exclude the case $\mathrm{lt}(f) = t$. But in this case $\mathrm{lt}(g) = t$ as well such that

$$\begin{aligned} f &= a + bs + ct \\ g &= u + vs + wt \end{aligned}$$

for some coefficients a, b, c, u, v and $w \in \mathbb{R}$. From this we may compute fg and compare its coefficients with those of p. Doing this an easy computation yields

(1)	au	=	-1	constant term
(2)	$av + bu$	=	0	s-term
(3)	$aw + cu$	=	0	t-term
(4)	bv	=	1	s^2-term
(5)	$bw + cv$	=	0	st-term
(6)	cw	=	1	t^2-term

In particular $a \neq 0$ and hence we may regard $(f/a)(ag) = fg = p$ instead. That is we may assume $a = 1$, then $u = -1$ by (1). And thus (2) turns into $b = v$ and (3) becomes $c = w$. From this and (5) we get $2bc = 0$. That is $b = 0$ or $c = 0$. But $b = 0$ would be a contradiction to (4) and $c = 0$ would be a contradiction to (6). Thus $\mathrm{lc}(f) = t$ cannot occur and this is the irreducibility of p.

- We now prove that $R = \mathbb{R}[s,t]/\mathfrak{p}$ is no UFD. To do this let us denote the set $X := \{\, (x,y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1 \,\}$. And thereby we define the following multiplicatively closed subset of R

$$U \;:=\; \{\, f + \mathfrak{p} \in R \mid \forall\, (x,y) \in X \,:\, f(x,y) \neq 0 \,\}$$

 By construction it is clear that U is truly well defined (if $f - g = q \in \mathfrak{p}$ then for any $(x,y) \in X$ we get $f(x,y) = g(x,y) + q(x,y) = g(x,y)$) and multiplicatively closed (as $\mathbb{R}$ is an integral domain). Let us now denote the element $r := s + \mathfrak{p} \in R$. Then we will prove that $r/1 \in U^{-1}R$ is irreducible but not prime. Thus $U^{-1}R$ is no UFD and hence R has not been an UFD by virtue of (2.131).

- Let us first prove that $r/1$ is not prime. To do this let us define the following elements $a := 2(t+1) + \mathfrak{p}$ and $b := -2(t-1) + \mathfrak{p} \in R$. Then $ab = -4(t^2-1) + \mathfrak{p} = 4s^2 + \mathfrak{p} = 4r^2$. In particular $r \mid ab$ and hence $r/1 \mid (ab)/1 = (a/1)(b/1)$. Now assume $r/1 \mid a/1$ that is there are some $h + \mathfrak{p} \in R$ and $u + \mathfrak{p} \in U$ such that $a/1 = (r/1)(h + \mathfrak{p}/u + \mathfrak{p})$. As $\mathbb{R}[s,t]$ is an integral domain that is $2(t+1)u + \mathfrak{p} = sh + \mathfrak{p}$ or in other words $2(t+1)u - sh =: q \in \mathfrak{p}$. Now regard $(0,1) \in X$ then $0 = q(0,1) = 4u(0,1) \neq 0$, a contradiction. That is $r/1 \not| \; a/1$ and likewise we find $r/1 \not| \; b/1$ by regarding $(0,-1) \in X$.

- So it only remains to prove that $r/1$ is irreducible. Thus suppose there are some $f, g \in \mathbb{R}[s,t]$ and $u + \mathfrak{p}$, $v + \mathfrak{p} \in U$ such that

$$\frac{s+\mathfrak{p}}{1} \;=\; \frac{r}{1} \;=\; \frac{f+\mathfrak{p}}{u+\mathfrak{p}}\frac{g+\mathfrak{p}}{v+\mathfrak{p}} \;=\; \frac{fg+\mathfrak{p}}{uv+\mathfrak{p}}$$

 That is $suv + \mathfrak{p} = fg + \mathfrak{p}$ or in other words $suv - fg =: q \in \mathfrak{p}$. As $q \in \mathfrak{p} = p\mathbb{R}[s,t]$ and p vanishes on X identically, so does q. And this means that for any $(x,y) \in X$ we have the following identity

$$xu(x,y)v(x,y) \;=\; f(x,y)g(x,y)$$

 In particular fg and suv and have the same roots. And as u, v do not vanish on X these are precisely the points $(0,1)$ and $(0,-1) \in X$. If f does not vanish on X then $f + \mathfrak{p} \in U$ and hence $f + \mathfrak{p}/u + \mathfrak{p}$ is a unit of $U^{-1}R$. Likewise if g does not vanish on X then $g + \mathfrak{p}/v + \mathfrak{p}$ is a unit of $U^{-1}R$. Thus in order to prove the irreducibility of $r/1$ it suffices to check that at f or g does not vanish on X.

- Thus assume this was false, that is f and g vanish on at least one point, say $f(0,1) = 0$ and $g(0,-1) = 0$ (else interchange f and g). We now parametrisize X using the following curve

$$\Omega \,:\, [0,2\pi] \twoheadrightarrow X \,:\, \omega \mapsto \begin{pmatrix} \cos(\omega) \\ \sin(\omega) \end{pmatrix}$$

 First suppose neither $f(0,-1) = 0$ nor $g(0,1) = 0$, that is f and g both have precisely one root on X. Then f cannot change signs on X (else $[0,2\pi] \to \mathbb{R} : \omega \mapsto f\Omega(\omega)$ would have to

have at least two roots because of $f\Omega(0) = f\Omega(2\pi) \neq 0$). And the same is true for g. Thus $(x,y) \mapsto f(x,y)g(x,y)$ *does not* change sign on X. Likewise uv does not have a single root on X and hence its sign on X is constant. Hence $(x,y) \mapsto xu(x,y)v(x,y)$ *does* change sign in contradiction to the equality of these two functions. Thus at least one of the two f or g even has to have two roots on X.

- We only regard the case $f(0,1) = 0$ and $g(0,1) = 0 = g(0,-1)$. The other case (where f has both roots) is completely analogous. The basic ideas is the following: as both f and g vanish in $(0,1)$ this is a root of order 2 for fg. But xuv only has a root of order 1 in $(0,1)$. Thus let us do same basic calculus - we have $\Omega(\pi/2) = (0,1)$ and in this point we get $\Omega'(\pi/2) = (1,0)$. Thus in this case we find another contradiction to $suv = fg$ by evaluating

$$\begin{aligned}\big((suv)\Omega\big)'(\pi/2) &= \langle \begin{pmatrix} uv + sv\partial_s u + su\partial_s v \\ sv\partial_t u + su\partial_t v \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \mid \begin{pmatrix} 1 \\ 0 \end{pmatrix} \rangle \\ &= u(0,1)v(0,1) \neq 0\end{aligned}$$

$$\begin{aligned}\big((fg)\Omega\big)'(\pi/2) &= \langle \begin{pmatrix} g\partial_s f + g\partial_s g \\ g\partial_t f + g\partial_t f \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \mid \begin{pmatrix} 1 \\ 0 \end{pmatrix} \rangle \\ &= \langle (0,0) \mid (1,0) \rangle = 0\end{aligned}$$

Proof of (2.71):

(ii) First consider $a > 0$, then it is clear that $q := b \operatorname{div} a \in \mathbb{Z}$ exists, as the set $\{q \in \mathbb{Z} \mid aq \leq b\} =]-\infty, b/a] \cap \mathbb{Z}$ contains the maximal element $q = a/b$ rounded down. And from the construction of $r := b \bmod a$ it is clear that $b = aq + r$. From the definition of q it is also clear that $0 \leq r$. Now assume $r \geq a$ then $a(q+1) = aq + a \leq aq + r = b$ and hence q would not have been maximal - a contradiction. Thus we also have $0 \leq r < a$ and hence $\alpha(r) = r < a = \alpha(a)$. Thus we have established the division with remainder for $a > 0$. If conversely $a < 0$ then $-a > 0$ and hence we may let $q := (-b) \operatorname{div} (-a)$ and $r := -((-b) \operatorname{div} (-a))$. Then we have just proved $-b = q(-a) - r$ which yields $b = qa + r$ and $\alpha(r) = \alpha(-r) < \alpha(-a) = \alpha(a)$.

(iii) Consider any $g \in E[t]$, $0 \neq f \in E[t]$ and let $\alpha := \operatorname{lc}(f)$. Then $\overline{f} := \alpha^{-1} f \in E[t]$ is normed. Further let $\overline{g} := \alpha^{-1} g$. Then by (2.67) there are $q, r \in E[t]$ such that $\overline{g} = q\overline{f} + r$. Multiplying with α we find $g = qf + \alpha r$ and $\deg(\alpha r) = \deg(r) < \deg(f)$ (as $\alpha \in E^*$). Thus we have established the division with remainder on $E[t]$.

(iv) It is straightforward to check that $\mathbb{Z}[\sqrt{d}]$ truly is a sub-ring of $\mathbb{C}$. Clearly $0 = 0 + 0\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ and $1 = 1 + 0\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Now consider $x = a + b\sqrt{d}$ and $y = f + g\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Then it is clear that

$$\begin{aligned} x + y &= (a+f) + (b+g)\sqrt{d} \quad \in \mathbb{Z}[\sqrt{d}] \\ xy &= (af + dbg) + (ag + bf)\sqrt{d} \quad \in \mathbb{Z}[\sqrt{d}] \end{aligned}$$

Thus $\mathbb{Z}[\sqrt{d}]$ is a sub-ring of $\mathbb{C}$ and in particular an integral domain. Now assume $x = y$, then we wish to verify $(a,b) = (f,g)$ (the converse implication is clear). Assume we had $b \neq g$ then we

would be able to divide by $b-g \neq 0$ and hence get

$$\sqrt{d} \;=\; \frac{f-a}{b-g} \;\in\; \mathbb{Q}$$

a contradiction to the assumption $\sqrt{d} \notin \mathbb{Q}$. Thus we have $b = g$ and hence (substracting $b\sqrt{d} = g\sqrt{d}$) also $a = f$. Thus $x \mapsto \overline{x}$ is truly well defined and the bijectivity is clear. We also see $\overline{0} = 0 - 0\sqrt{d} = 0$ and $\overline{1} = 1 - 0\sqrt{d} = 1$ immediately. It remains to prove that $x \mapsto \overline{x}$ also is additive and multiplicative, by computing

$$\overline{x} + \overline{y} \;=\; (a - b\sqrt{d}) + (f - g\sqrt{d}) \;=\; (a+f) - (b+g)\sqrt{d}) \;=\; \overline{x+y}$$

$$\overline{xy} \;=\; (a - b\sqrt{d})(f - g\sqrt{d}) \;=\; (af + dbg) - (ag + bf)\sqrt{d} \;=\; \overline{xy}$$

But from this it is clear that ν also is multiplicative. Just compute $\nu(xy) = |xy\overline{xy}| = |x\overline{x}y\overline{y}| = |x\overline{x}| \cdot |y\overline{y}| = \nu(x)\nu(y)$. We finally note that for any $0 \neq x \in \mathbb{Z}[\sqrt{d}]$ we get $\nu(x) \neq 0$, since $\nu(x) = |a^2 - db^2| = 0$ is equivalent to $a^2 = db^2$. Thus if $b = 0$ then $a = 0$ and hence $x = 0$ as claimed. And if $b \neq 0$ then we may divide by b to find $(a/b)^2 = d$. In other words $\sqrt{d} = a/b \in \mathbb{Q}$, a contradiction to the assumption $\sqrt{d} \notin \mathbb{Q}$. Thus the case $b \neq 0$ cannot occur in the first place.

Next we prove that the units of $\mathbb{Z}[\sqrt{d}]$ are precisely the elements x such that $\nu(x) = 1$. If $x \in \mathbb{Z}[\sqrt{d}]^*$ is a unit, then we have $1 = \nu(1) = \nu(xx^{-1}) = \nu(x)\nu(x^{-1})$ and hence $\nu(x) \in \mathbb{Z}^*$. But as also $\nu(x) \geq 0$ this yields $\nu(x) = 1$. Thus consider any $x = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ such that $\nu(x) = 1$. Then $x\overline{x} = a^2 - db^2 = \pm 1$ and hence $x^{-1} = \pm\overline{x}$ is invertible.

Now assume that $d \leq -3$ then we want to prove that 2 is an irreducible element of $\mathbb{Z}[\sqrt{d}]$ that is not prime. We begin by proving that 2 is not prime: as either d or $d-1$ is even we have

$$2 \mid d(d-1) \;=\; d^2 - d \;=\; (d + \sqrt{d})(d - \sqrt{d})$$

but we have $2 \nmid d \pm \sqrt{d}$, because if we assume $2(a + b\sqrt{d}) = d \pm \sqrt{d}$ then (comparing the $\sqrt{d}$-coefficient) we had $2b = \pm 1 \in \mathbb{Z}$ in contradiction to $2 \notin \mathbb{Z}^*$. However 2 is irreducible, assume $2 = xy$ for some $x, y \in \mathbb{Z}[\sqrt{d}]$. Then $4 = \nu(2) = \nu(xy) = \nu(x)\nu(y)$. Hence we have $\nu(x) \in \{1, 2, 4\}$. If $\nu(x) = 1$ then $x \in \mathbb{Z}[\sqrt{d}]^*$ is a unit. And if $\nu(x) = 4$ then $\nu(y) = 1$ and hence $y \in \mathbb{Z}[\sqrt{d}]^*$ is a unit. It suffices to exclude the case $\nu(x) = 2$, that is assume $\nu(x) = 2$. As $d \leq -3$ we have $2 = \nu(x) = a^2 - db^2$. Thus in the case $b \neq 0$ we obtain $2 = a^2 - db^2 \geq 0 + 3 \cdot 1 = 3$ a contradiction. And in case $b = 0$ we get $2 = a^2$ for some $a \in \mathbb{Z}$, in contradiction to the irreducibility of 2 in $\mathbb{Z}$. Thus $\nu(x) = 2$ cannot occur and this means that $2 \in \mathbb{Z}[\sqrt{d}]$ is irreducible.

It remains to prove that $(\mathbb{Z}[\sqrt{d}], \nu)$ even is an Euclidean domain for $d \in \{-2, -1, 2, 3\}$. We consider the elements $0 \neq x = a + b\sqrt{d}$ and $y = f + g\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, then (as $\nu(y) \neq 0$) we may define

$$\begin{aligned} p &:= \frac{af - dbg}{a^2 - db^2} \\ q &:= \frac{ag - bf}{a^2 - db^2} \end{aligned}$$

That is $p + q\sqrt{d} := (1/(a^2 - db^2))y\overline{x}$. And therefore we obtain the identity $(p + q\sqrt{d})x = (1/(f^2 - dg^2))y\overline{x}x = y$. In other words we have found y/x to be $p + q\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$. Now choose

$r, s \in \mathbb{Z}$ such that $|p-r|$ and $|q-s| \leq 1/2$ (which is possible, as the intervals $[r-1/2, r+1/2]$ (for $r \in \mathbb{Z}$) cover $\mathbb{Q}$) and define

$$\begin{aligned} u &:= r + s\sqrt{d} \\ v &:= y - ux \end{aligned}$$

Then it is clear that $u, v \in \mathbb{Z}[\sqrt{d}]$ and $y = ux + v$. But further we find

$$x\big((p-r) + (q-s)\sqrt{d}\big) = x\left(\frac{y}{x} - u\right) = y - ux = v$$

Due to the multiplicativity of ν (which even remains true for coefficients (here $p-r$ and $q-s$) in $\mathbb{Q}$) we find $\nu(v) = \nu(x)|(p-r)^2 - d(q-s)^2|$. But as $|d| \leq 3$ we can estimate

$$|(p-r)^2 - d(q-s)^2| \;\leq\; (p-r)^2 + |d|(q-s)^2 \;\leq\; (1/2)^2 + 3(1/2)^2 \;=\; 1$$

The case $|(p-r)^2 - d(q-s)^2| = 1$ can only occur if $|p-r| = |p-s| = 1/2$ and $d = 3$. But in this case we have $|(p-r)^2 - d(q-s)^2| = |1/4 - 3/4| = 1/2 < 1$. Thus we have even proved the strict estimate

$$\nu(v) \;=\; \nu(x)|(p-r)^2 - d(q-s)^2| \;<\; \nu(x)$$

Altogether we have seen that $\mathbb{Z}[\sqrt{d}]$ is an integral domain and that given $0 \neq x, y \in \mathbb{Z}[\sqrt{d}]$ we can find $u, v \in \mathbb{Z}[\sqrt{d}]$ such that $y = ux + v$ and $\nu(v) < \nu(x)$. But this is the condition to be an Euclidean domain.

□

Proof of (2.72):

- Without loss of generality we assume $\nu(a) \leq \nu(b)$ and let $f_1 := b$ and $f_2 := a$. That is if f and g are determined using the initialisation of the algorithm, then we get $f_1 = g$ and $f_2 = f$. Suppose we have already computed $f_1, \ldots, f_k \in R$ and $f_k \neq 0$, then in the next step the algorithm computes $q_k := q$ and $f_{k+1} := r \in R$ such that

$$f_{k-1} \;=\; q_k f_k + f_{k+1}$$

and $\nu(f_{k+1}) < \nu(f_k)$. Thus by induction on k we find the following strictly decreasing sequence of natural numbers

$$\nu(b) \;=\; \nu(f_1) \;\geq\; \nu(f_2) \;>\; \nu(f_3) \;>\; \ldots \;>\; \nu(f_k) \;>\; \nu(f_{k+1}) \;>\; \ldots$$

As $\nu(b)$ is finite this chain cannot decrease indefinitely but has to terminate at some level n. That is $f = f_{n+1} = 0$. And therefore $f_{n-1} = q_n g$ where $g = f_n$.

- We will now prove that for any $1 \leq k \leq n$ we have $g \mid f_k$. For $k = n$ we trivially have $g \mid g = f_n$. And for $k = n-1$ we have $f_{n-1} = q_n g$ by construction. Thus by induction we can assume $k \leq n-1$ and $g \mid f_n$ to $g \mid f_k$. Then from $f_{k-1} = q_k f_k + f_{k+1}$ it also is clear that $g \mid f_{k-1}$ completing the induction. In particular we have $g \mid f_2 = a$ and $g \mid f_1 = b$.

- Now suppose we are given some $d \in R$ with $d \mid a = f_2$ and $d \mid b = f_1$. Then we will prove that for any $k \in 1 \ldots n$ we get $d \mid f_n$ by induction on k. Thus assume $k \geq 2$ and $d \mid f_1$ to $d \mid f_k$. Then from $f_{k+1} = f_{k-1} + q_k f_k$ we also get $d \mid f_{k+1}$ completing the induction. In particular we get $d \mid f_n = g$. And hence g truly is the greatest common divisor of a and b.

- We will now prove the correctness of the refined Euclidean algorithm. The first part (the computation of g) is just a reformulation of the standard Euclidean algorithm. And as the second part is a finite computation, it is clear that the algorithm terminates. Next we will first prove that for any $2 \leq k \in \mathbb{N}$ we have $f_k = r_k f_2 + s_k f_1$. For $k = 2$ this is trivial $f_2 = 1 \cdot f_2 + 0 \cdot f_1 = r_2 f_2 + s_2 f_1$. And for $k \geq 3$ we have computed $q_k \in R$ such that $f_{k-1} = q_k f_k + f_{k+1}$ for some $f_{k+1} \in R$. In particular $f_3 = f_1 - q_2 f_2 = (-q_2) f_2 + 1 \cdot f_1 = r_3 f_2 + s_3 f_1$. Now we will use induction on k. That is we assume $f_{k-1} = r_{k-1} f_2 + s_{k-1} f_1$ and $f_k = r_k f_2 + s_k f_1$. Then a computation immediately yields

$$\begin{aligned} r_{k+1} f_2 + s_{k+1} f_1 &= (r_{k-1} - q_k r_k) f_2 + (s_{k-1} - q_k s_k) f_1 \\ &= (r_{k-1} f_2 + s_{k-1} f_1) - q_k (r_k f_2 + s_k f_1) \\ &= f_{k-1} - q_k f_k \;=\; f_{k+1} \end{aligned}$$

 In particular for $k = n$ we find $g = f_n = r_n f_2 + s_n f_1$. Thus let us distinguish the two cases. If $\nu(a) \leq \nu(b)$ we have $f_1 = b$, $f_2 = a$, $r = r_n$ and $s = s_n$. Thereby we get $g = r_n f_2 + s_n f_1 = ra + sb$. And conversely if $\nu(a) > \nu(b)$ then $f_1 = a$, $f_2 = b$, $r = s_n$ and $s = r_n$. Thereby we get $g = r_n f_2 + s_n f_1 = sb + ra$. Thus in any case we have obtained r and $s \in R$ such that $g = ra + sb$.

□

Proof of (2.76):

(i) We use induction on n to prove the statement. For $n = 0$ and any $a \in R_0 = R^*$ it is clear that $a \in R_1$, as for any $b \in R$ we may choose $r = 0$ and thereby get $a(ba^{-1}) = b$ such that $a \mid b - r$. Thus for $n \mapsto n + 1$ we are given $a \in R_n$ and any $b \in R$. That is we have $a \mid b - r$ for some $r \in R_{n-1}$. But by induction hypothesis we know $R_{n-1} \subseteq R_n$ and hence $r \in R_n$. But this again means $a \in R_{n+1}$ (as b has been arbitrary) which had to be proved.

(ii) We use induction on n again. For $n = 0$ we are given any $a \in R$ such that $\nu(a) \leq 0$. If $\nu(a) < 0$ then $\nu(a) = -\infty$ and hence $a = 0$. Otherwise $\nu(a) = 0$ and we use division with remainder to find some q, $r \in R$ such that $1 = qa + r$ and $\nu(r) < \nu(a) = 0$. But this can only be if $\nu(r) = -\infty$ which is $r = 0$. Hence we have $1 = qa$, that is $a \in R^* = R_0$ is a unit of R. In the induction step $n \mapsto n + 1$ we are given some $a \in R$ with $\nu(a) \leq n + 1$. Given $b \in R$ we use division with remainder to find q, $r \in R$ such that $b = qa + r$ and $\nu(r) < \nu(a) \leq n + 1$. Thus we have $\nu(r) \leq n$ and by induction hypothesis this yields $r \in R_n \cup \{0\}$. That is $a \mid b - r$ for some $r \in R_n \cup \{0\}$. And as b has been arbitrary this means $a \in R_{n+1}$, which had to be shown.

(iii) Clearly μ is well defined, as by assumption any $0 \neq a \in R$ is contained in some R_n. We need to prove that μ truly allows division with remainder: thus consider any $0 \neq a$ and $b \in R$, then we need to find q, $r \in R$ such that $b = qa + r$ and $\mu(r) < \mu(a)$. If $\mu(a) = 0$ then $a \in R_0 = R^*$ and hence we may choose $q := ba^{-1}$ and $r = 0$. If $\mu(a) \geq 1$ then we let $n := \mu(a) - 1 \in \mathbb{N}$. As $a \in R_{n+1}$ and $b \in R$ we have $a \mid b - r$ for some $r \in R_n \cup \{0\}$. This again yields $\mu(r) \leq n < n + 1 = \mu(a)$ and $b = qa + r$ for some $q \in R$, just what we wanted.

(iii) Next we want to prove $\mu(a) \leq \mu(ab)$. If $ab = 0$ then (as $b \neq 0$ and R is an itegral domain) we have $a = 0$. Thereby $\mu(a) = -\infty = \mu(ab)$. Thus assume $ab \neq 0$, and let $n := \mu(ab) \in \mathbb{N}$. If $n = 0$ then $ab \in R_0 = R^*$ and hence $a \in R^* = R_0$ (with $a^{-1} = b(ab)^{-1}$). Thus we likewise have $\mu(a) = 0 = \mu(ab)$. If now $n \geq 1$ then for any $c \in R$ there is some $r \in R_{n-1} \cup \{0\}$ such that $ab \mid c - r$. But as $a \mid ab$ this yields $a \mid c - r$, too and hence $a \in R_n$ again. Thereby $\mu(a) \leq n = \mu(ab)$.

(iii) If $a \in R^*$ then by (iii) above we have $\mu(b) \leq \mu(ab) \leq \mu(a^{-1}ab) = \mu(b)$ and hence $\mu(b) = \mu(ab)$. Conversely suppose $\mu(b) = \mu(ab)$. As $b \neq 0$ we also have $ab \neq 0$ (else $\mu(ab) = -\infty \neq \mu(b)$). Thus we may use division with remainder to find some q, $r \in R$ such that $b = q(ab) + r$ and $\mu(r) < \mu(b)$. Rearranging this equation we find $(1 - qa)b = r$. Now suppose we had $1 - qa \neq 0$, then by (iii) above again we had $\mu(b) \leq \mu((1 - qa)b) = \mu(r) < \mu(b)$, a contradiction. Thus we have $qa = 1$ and this means $a \in R^*$ as claimed.

(iv) If $R \setminus \{0\} = \bigcup_n R_n$ then (R, μ) is an Euclidean domain by (iii). Conversely suppose (R, ν) is an Euclidean domain for some Euclidean function ν. Now consider any $0 \neq a \in R$, and let $n := \nu(a)$. Then we have already seen in (ii) that $a \in R_n$ and hence we have $R \setminus \{0\} = \bigcup_n R_n$.

(v) As (R, ν) is an Euclidean domain we have $R \setminus \{0\} = \bigcup_n R_n$ by (iv). But by (iii) this implies that (R, μ) is an Euclidean domain, too. Thus consider any $a \in R$, if $a = 0$ then $\mu(a) = -\infty = \nu(a)$ by convention. Else let $n := \nu(a) \in \mathbb{N}$. Then $a \in R_n$ by (ii) and hence $\mu(a) \leq n = \nu(a)$ by construction of μ.

□

Proof of (2.79):
We will only prove parts (i), (ii) and (iii) here. Part (iv) requires the theory of Dedekind domains an will be postponed until then - see page (1118).

(i) Clearly $0 \trianglelefteq_{\mathfrak{i}} R$ is a prime ideal, as R is an integral domain (if $ab \in 0$ then $ab = 0$ and hence $a = 0$ or $b = 0$ such that $a \in 0$ or $b \in 0$ again). And further any maximal ideal is prime, because of (2.24). Conversely consider any non-zero prime ideal $0 \neq \mathfrak{p} \trianglelefteq_{\mathfrak{i}} R$. As R is a PID there is some $p \in R$ such that $\mathfrak{p} = pR$. By (2.58.(ii)) this means that p is prime and due to (2.58.(v)) this implies that p is irreducible (as R is an integral domain). Now consider any ideal $\mathfrak{a}$ such that $\mathfrak{p} \subseteq \mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$. As R is a PID there is some $a \in R$ with $\mathfrak{a} = aR$ again. Now $p \in pR \subseteq aR$ means that there is some $b \in R$ such that $p = ab$. But p has been irreducible, that is $a \in R^*$ or $b \in R^*$. In the case $a \in R^*$ we have $\mathfrak{a} = aR = R$. And in the case $\mathfrak{b} \in R^*$ we have $a \approx b$ and hence $\mathfrak{a} = aR = pR = \mathfrak{p}$. As $\mathfrak{a}$ has been arbitrary this means that $\mathfrak{p}$ already is maximal.

(ii) As R is a PID every ideal $\mathfrak{a}$ of R is generated by *one* element $\mathfrak{a} = aR$. In particular any ideal $\mathfrak{a}$ is generated by *finitely many* elements. Thus R is notherian by property (c) in (2.34). We will now prove property (d) of UFDs. As R is noetherian property (1) in (2.60.(d)) is trivially satisfied by (ACC) of noetherian rings. Hence it suffices to check property (2) of (2.60.(d)). But as R is an integral domain any prime element $p \in R$ already is irreducible, due to (2.58.(ii)). This leaves

$$p \in R \text{ irreducible} \quad \Longrightarrow \quad p \in R \text{ prime}$$

Thus suppose $p \mid ab$ for some p, a and $b \in R$, say $pq = ab$. As R is a PID and $aR + pR \trianglelefteq_{\mathfrak{i}} R$ is an ideal we find some $d \in R$ such that $dR = aR + pR$. That is there are r, $s \in R$ such that $d = ar + ps$. And as $a \in aR + pR = dR$ there is some $f \in R$ with $a = df$. Likewise we find some $g \in R$ with $p = dg$. But as p is irreducible we have $g \in R^*$ or $d \in R^*$. If $g \in R^*$ then we get $p \mid a$ from

$$p(fg^{-1}) \;=\; (g^{-1}p)f \;=\; df \;=\; a$$

And if $d \in R^*$ we get $p \mid b$ by the equalities below. Thus we have found $p \mid a$ or $p \mid b$ which means that p is prime

$$\begin{aligned} p(d^{-1}qr + d^{-1}bs) \;&=\; d^{-1}(pqr + pbs) \;=\; d^{-1}(abr + pbs) \\ &=\; bd^{-1}(ar + ps) \;=\; bd^{-1}d \;=\; b \end{aligned}$$

(iii) If $\mathfrak{a} = 0$ then $\mathfrak{a} = 0R$ is a principal ideal (generated by $0 \in R$). And if $\mathfrak{a} \neq 0$ there is some $0 \neq b \in \mathfrak{b}$. Therefore we may choose a as given in the claim of (iii). Now consider any $b \in \mathfrak{a}$ and choose q, $r \in R$ such that $b = qa + r$ and $\nu(r) < \nu(a)$. Then $r = b - qa \in \mathfrak{a}$ (as a, $b \in \mathfrak{a}$). But a has minimal value $\nu(a)$ among all those $b \in \mathfrak{a}$ with $b \neq 0$. Therefore $r \in \mathfrak{a}$ and $\nu(r) < \nu(a)$ implies $r = 0$. Thus $b = qa \in aR$, and as b has been arbitrary this means $\mathfrak{a} \subseteq aR$. And as $a \in R$ we have $aR \subseteq \mathfrak{a}$. Together we find that $\mathfrak{a} = aR$ is a principal ideal. And as $\mathfrak{a}$ has been arbitrary this means that R is a PID.

□

Proof of (2.80):

- Let us prove this statement by induction on n, starting with $n = 1$. Clearly $\mathfrak{m} := tF[t] \trianglelefteq_{\mathfrak{i}} F[t]$ is a maximal ideal, as $F[t]/\mathfrak{m} \xrightarrow{\sim} F$ are isomorphic under $f + \mathfrak{m} \mapsto f(0)$. Thus $F[t]/\mathfrak{m}$ is a field and thereby $\mathfrak{m}$ a maximal ideal. Thus $F[t]$ has at least one maximal ideal.

- Suppose $F[t]$ only had finitely many ideals, say $\mathrm{Smax}(F[t]) = \{\, \mathfrak{m}_1, \ldots, \mathfrak{m}_n \,\}$ are all of them. By (2.79.(iii)) $F[t]$ is a PID, as it is an Euclidean domain under the degree function. So any $\mathfrak{m}_i$ is generated by a single element $\mathfrak{m}_i = p_i F[t]$. As any maximal ideal $\mathfrak{m}_i$ is prime, the p_i are prime elements of $F[t]$. Now define

$$g \;:=\; p_1 \ldots p_n + 1 \;\in\; F[t]$$

As p_i is prime it is non-zero and not a unit. As $F[t]^* = F^*$ together this means $\deg(p_i) \geq 1$, and therefore $\deg(g) = \deg(p_1) + \cdots + \deg(p_n) \geq 1$. In particular $g \in F[t] \setminus F$ is non-zero and not a unit. As $F[t]$ is a PID and therefore an UFD, g admits a prime divisor, i.e. there is a prime element $p \in F[t]$ with $p \mid g$. That is there is some $h \in F[t]$ with $ph = g = p_1 \ldots p_n + 1$. Suppose we had $p = ap_1$ for some $a \in F^*$, then $ap_1 h = ph = p_1 \ldots p_n + 1$ such that $p_1(ah - p_2 \ldots p_n) = 1$. This would mean $p_1 \in F[t]^*$ in contradiction to p_1 being a prime element. Therefore p is not associate to p_1 and similarly not to any of the p_i. That is $pF[t]$ is an ideal, different from $\mathfrak{m}_1$ to $\mathfrak{m}_n$. But p is a prime element and hence $pF[t]$ is a non-zero prime ideal. By (2.79.(i)) this means $pF[t]$ is a maximal ideal. But this contradicts $\{\, \mathfrak{m}_1, \ldots, \mathfrak{m}_n \,\}$ to be a complete list of maximal ideals of $F[t]$. Therefore $F[t]$ has infinitely many maximal ideals.

- Now for the induction step: By induction hypothesis we know that $R := F[t_1, \ldots, t_n]$ has finitely many maximal ideals. We have to check that $F[t_1, \ldots, t_{n+1}] = R[t_{n+1}]$ has infinitely many prime ideals, as well. Let us abbreviate $t := t_{n+1}$, and pick up any maximal ideal in R. Then

$$\widetilde{\mathfrak{m}} \;:=\; \mathfrak{m} + tR[t] \;=\; \{\, f \in R[t] \mid f(0) \in \mathfrak{m} \,\}$$

gives rise to an isomorphism $R[t]/\widetilde{\mathfrak{m}} \xrightarrow{\sim} R/\mathfrak{m}$ of R-algebras, according to (3.43.(iv)). But $R/\mathfrak{m}$ is a field, as $\mathfrak{m}$ is a maximal ideal and thereby $R[t]/\widetilde{\mathfrak{m}}$ is a field, which means $\widetilde{\mathfrak{m}} \trianglelefteq_{\mathrm{i}} R[t]$ is a maximal ideal. These ideals are pairwise distinct: If $\mathfrak{m}$ and $\mathfrak{n} \trianglelefteq_{\mathrm{i}} R$ are maximal ideals with $\widetilde{\mathfrak{m}} = \widetilde{\mathfrak{n}}$, then we get $\mathfrak{m} = \widetilde{\mathfrak{m}} \cap R = \widetilde{\mathfrak{n}} \cap R = \mathfrak{n}$. Thus we have an injective map

$$\mathrm{Smax}(R) \;\hookrightarrow\; \mathrm{Smax}(R[t]) \;:\; \mathfrak{m} \mapsto \widetilde{\mathfrak{m}}$$

That is $F[t_1, \ldots, t_{n+1}] = R[t]$ has as least as many maximal ideals, as $R = F[t_1, \ldots, t_n]$. In particular, as $\mathrm{Smax}(R)$ is infinite by induction hypothesis, $\mathrm{Smax}(R[t])$ is infinite, as well.

□

Proof of (2.82):

(i) As R is an UFD by (2.79.(ii)) the length $\ell(a) \in \mathbb{N}$ of $0 \neq a \in R$ is well defined, due to (2.60.(b)). Therefore $\delta : R \to \mathbb{N}$ is a well-defined function and it is clear that it satisfies properties (1) and (2). Thus consider any $0 \neq a, b \in R$, as R is a PID we may choose some $r \in R$ such that $rR = aR + bR$. It is clear that $r \neq 0$, as $0 \neq a \in rR$. Now suppose $b \notin aR$, Then it is clear that $r \in aR + bR$ and it remains to prove $\delta(r) < \delta(a)$. As $a \in aR + bR = rR$ there is some $s \in R$ such that $a = rs$. Suppose $s \in R^*$, then $a \approx r$ and hence $aR = rR$. But $b \in aR + bR = rR = aR$ is a contradiction to $b \notin aR$. Thus $s \notin R^*$ which means $\ell(s) \geq 1$. Hence we have $\delta(s) \geq 2$ and as $\delta(r) > 0$ (recall $r \neq 0$) this finally is

$$\delta(r) \;<\; 2\delta(r) \;\leq\; \delta(r)\delta(s) \;=\; \delta(rs) \;=\; \delta(a)$$

(ii) As $\mathfrak{a} \neq 0$ there is some $0 \neq b \in \mathfrak{a}$. And hence we may choose $a \in \mathfrak{a}$ as given in the claim of (ii). We now want to verify $\mathfrak{a} = aR$, as $a \in \mathfrak{a}$ the inclusion $aR \subseteq \mathfrak{a}$ is clear. Conversely choose any $0 \neq b \in \mathfrak{a}$ ($0 \in aR$ is clear). If we had $b \notin aR$, then by property (3) there would be some $r \in aR + bR$ such that $\delta(r) < \delta(a)$. But as $a, b \in \mathfrak{a}$ we have $aR + bR \subseteq \mathfrak{a}$ and hence $r \in \mathfrak{a}$. As a has been chosen to have minimal value $\delta(a)$ this only leaves $r = 0$ and hence $0 \neq a \in aR + bR = rR = 0$, a contradiction. Thus we have $b \in aR$ and hence $\mathfrak{a} \subseteq aR$ as well.

(iii) By construction of δ it is clear that $\delta : R \to \mathbb{N}$ and that δ satisfies (2). It remains to verify (3), thus consider any $0 \neq a, b \in R$ then we choose $q, r \in R$ such that $b = qa + r$ and $\nu(r) < \nu(a)$. If $r = 0$ then $b = qa \in aR$. And if $r \neq 0$ we have $r = -qa + b \in aR + bR$ and $\delta(r) = \nu(r) + 1 < \nu(a) + 1 = \delta(a)$.

□

Proof of (2.83):

(i) First suppose $mR = \bigcap_a aR$, in particular $mR \subseteq aR$ for any $a \in R$. But this is $a \mid m$ for any $a \in A$ and hence $A \mid m$. Now consider any $n \in R$ such that $A \mid n$, that is $a \mid n$ and hence $n \in aR$

for any $a \in A$. Therfore $n \in \bigcap_a aR = mR$ and hence $m \mid n$. Thus we have proved $m \in \operatorname{lcm}(A)$. Conversely suppose $m \in \operatorname{lcm}(A)$, then $A \mid m$ and hence $m \in \bigcap_a aR$ again. In particular we have $mR \subseteq \bigcap_a aR$. Now consider any $n \in \bigcap_a aR$, then $A \mid n$ again and hence $m \mid n$ by assumption on m. Thus we have $n \in mR$ and as n has been arbitrary this is the converse inclusion $\bigcap_a aR \subseteq mR$.

(ii) Let $dR = \sum_a aR$ then for any $a \in A$ we have $aR \subseteq dR$ and hence $d \mid a$. Thus we found $d \mid A$, as a has been arbitrary. Now consider some $c \in R$ such that $c \mid A$. That is for any $a \in A$ we get $c \mid a$ and hence $aR \subseteq cR$. But from this we get $dR = \sum_a aR \subseteq cR$ which also is $c \mid d$. Together we have proved $d \in \gcd(A)$ again.

(iii) Now assume that R is a PID, then we will also prove the converse implication. By assumption on R there is some $g \in R$ such that $gR = \sum_a aR$ and by (ii) this means $g \in \gcd(A)$. Now from (2.58.(viii)) and d, $g \in \gcd(A)$ we get $d \approx g$ and hence $dR = gR = \sum_a aR$.

(iv) For $n = 1$ the statement is trivial for $b_1 := b$, thus let us assume $n \geq 2$. Then we denote $a := a_1 \dots a_n$ and $\widehat{a}_i := a/a_i \in R$. Now consider $d \in \gcd\{\widehat{a}_1, \dots, \widehat{a}_n\}$ and suppose we had $d \notin R^*$. Then (as R is an UFD) there would be a prime element $p \in R$ dividing $p \mid d$. Thus we had $p \mid d \mid \widehat{a}_1$ and hence (as p is prime) there would be some $i \in 2 \dots n$ such that $p \mid a_i$. Likewise for i we have $p \mid d \mid \widehat{a}_i$ and hence $p \mid a_j$ for some $j \neq i$. But a_i and a_j are relatively prime by assupmtion, a contradiction. Thus we have $d \in R^*$, that is $1 \in \gcd\{\widehat{a}_1, \dots, \widehat{a}_n\}$. And by (iii) this means that there are some $h_1, \dots, h_n \in R$ such that $1 = h_1\widehat{a}_1 + \dots + h_n\widehat{a}_n$. Now let $b_i := bh_i$, then the claim is immediate from

$$\sum_{i=1}^{n} \frac{b_i}{a_i} \;=\; \sum_{i=1}^{n} \frac{bh_i\widehat{a}_i}{a} \;=\; \frac{b}{a} \sum_{i=1}^{n} h_i\widehat{a}_i \;=\; \frac{b}{a}$$

□

Proof of (2.84):

- (a) $\implies$ (b): consider $a, b \in R$, by assumption there are $r, s \in R$ such that $d = ra + sb \in \gcd(a, b)$. By construction we have $d \in aR + bR$ and hence $dR \subseteq aR + bR$. On the other hand we have $d \in \gcd(a, b)$ and hence $d \mid a$ and $d \mid b$. But that is $aR \subseteq dR$ and $bR \subseteq dR$ such that $aR + bR \subseteq dR$ as well. Together that is $dR = aR + bR$.

- (b) $\implies$ (c): $\mathfrak{a}$ being finitely generated means that there are some $a_1, \dots, a_n \in R$ such that $\mathfrak{a} = a_1R + \dots + a_nR$. We will now use induction on n to prove that $\mathfrak{a}$ is principal. In the case $n = 0$ we have $\mathfrak{a} = 0 = 0R$ and in the case $n = 1$ trivially $\mathfrak{a} = a_1R$ is principal. Thus we may assume $n \geq 2$. Then by induction hypothesis $\mathfrak{u} := a_1R + \dots + a_{n-1}R \trianglelefteq_{\mathrm{i}} R$ is principal, that is there is some $u \in R$ such that $\mathfrak{u} = uR$. Now $\mathfrak{a} = a_1R + \dots + a_nR = \mathfrak{u} + a_nR = uR + a_nR$. Thus by assumption (b) there is some $d \in R$ such that $\mathfrak{a} = dR$ is principal.

- (c) $\implies$ (a): consider any $a, b \in R$ and let $\mathfrak{a} := aR + bR$. By construction $\mathfrak{a}$ is finitely generated and hence there is some $d \in R$ such that $\mathfrak{a} = dR$. Now $d \in aR + bR$ means that there are some r, $s \in R$ such that $d = ra + sb$. And by (2.83.(ii)) $dR = aR + bR$ yields that $ra + sb = d \in \gcd(a, b)$ as well.

□

Proof of (2.85):

- (a) $\implies$ (b) and (c): if R is a PID then R is a noetherian UFD due to (2.79.(ii)). And it is clear that R also is a Bezout domain (e.g. by property (c) in (2.84)).
- (c) $\implies$ (a): consider any ideal $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$, as R is noetherian $\mathfrak{a}$ is finitely generated, due to property (c) of noetherian rings (2.34). And due to poroperty (c) of Bezout domains (2.84) this means that $\mathfrak{a}$ is principal. As a Bezout domain also is an integral domain this means that R is a PID.
- (b) $\implies$ (a): consider any ideal $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$. If $\mathfrak{a} = 0$ then $\mathfrak{a} = 0R$ trivially is principal. Thus we assume $\mathfrak{a} \neq 0$ and choose any $0 \neq a \in R$ with

 $$\ell(a) \;=\; \min\{\, \ell(b) \mid 0 \neq b \in \mathfrak{a} \,\}$$

 where $\ell(a)$ is the number of prime factors of a, that is $\ell(a) = k$, where $a = p_1 \dots p_k$ for some prime elements $p_i \in R$. As $a \in \mathfrak{a}$ we have $aR \subseteq \mathfrak{a}$. Conversely consider any $0 \neq b \in \mathfrak{a}$. As R is a Bezout domain the ideal $aR + bR$ is principal $aR + bR = dR$ for some $d \in R$, due to property (b) in (2.84). As $a, b \in \mathfrak{a}$ we have $d \in aR + bR \subseteq \mathfrak{a}$ and clearly $d \neq 0$ (as $a \neq 0$). Thus by construction of a we have $\ell(a) \leq \ell(d)$. But on the other hand we have $a \in aR + bR = dR$ and hence $d \mid a$ which implies $\ell(d) \leq \ell(a)$ by (2.64.(iii)). But from $d \mid a$ and $\ell(a) = \ell(d)$ we get $a \approx d$ by choosing prime decompositions of a and d as in (2.64.(iv)). Therefore we have $b \in aR + bR = dR = aR$. This proves $b \in aR$ and hence $\mathfrak{a} \subseteq aR$, as b has been arbitrary ($b = 0$ is clear). Altogether we have $\mathfrak{a} = aR$ is principal and hence R is a PID, as $\mathfrak{a}$ has been arbitrary.

□

Proof of (2.88):

- (a) $\implies$ (b): consider $a + \mathfrak{a} \in \mathrm{zd}(R/\mathfrak{a})$, that is $a \in \mathrm{zd}_R(R/\mathfrak{a})$, then by assumption we have $a \in \sqrt{\mathfrak{a}}$. That is $a^k \in \mathfrak{a}$ for some $k \in \mathbb{N}$ and hence $(a + \mathfrak{a})^k = a^k + \mathfrak{a} = 0 + \mathfrak{a}$ such that $a + \mathfrak{a}$ is a nilpotent of $R/\mathfrak{a}$.
- (b) $\implies$ (c): the nil-radical of $R/\mathfrak{a}$ is trivially included in the set of zero-divisors of $R/\mathfrak{a}$ due to (1.47.(ii)), which implies equality.
- (c) $\implies$ (a): consider $a \in \mathrm{zd}_R(R/\mathfrak{a})$, that is $a + \mathfrak{a} \in \mathrm{zd}(R/\mathfrak{a})$. Then by assumption $a + \mathfrak{a}$ is a nilpotent of $R/\mathfrak{a}$, that is $a^k + \mathfrak{a} = (a + \mathfrak{a})^k = 0 + \mathfrak{a}$ for some $k \in \mathbb{N}$. But this again means $a^k \in \mathfrak{a}$ and hence $a \in \sqrt{\mathfrak{a}}$.
- (c) $\implies$ (d): consider $a, b \in R$ such that $ab \in \mathfrak{a}$ but $b \notin \mathfrak{a}$. That is $(a + \mathfrak{a})(b + \mathfrak{a}) = ab + \mathfrak{a} = 0 + \mathfrak{a}$ and as $b + \mathfrak{a} \neq 0 + \mathfrak{a}$ this means that $a + \mathfrak{a} \in \mathrm{zd}(R/\mathfrak{a})$ is a zero-divisor of $R/\mathfrak{a}$. By assumption this means that $a + \mathfrak{a}$ is a nilpotent of $R/\mathfrak{a}$ and hence $a^k + \mathfrak{a} = (a + \mathfrak{a})^k = 0 + \mathfrak{a}$ for some $k \in \mathbb{N}$. But this again is $a^k \in \mathfrak{a}$ and hence $a \in \sqrt{\mathfrak{a}}$.
- (d) $\implies$ (b): consider $a + \mathfrak{a} \in \mathrm{zd}R/\mathfrak{a}$ that is there is some $0 + \mathfrak{a} \neq b + \mathfrak{a} \in R/\mathfrak{a}$ such that $ab + \mathfrak{a} = (a + \mathfrak{a})(b + \mathfrak{a}) = 0 + \mathfrak{a}$. But this means $ab \in \mathfrak{a}$ and as also $b \notin \mathfrak{a}$ we find $a \in \sqrt{\mathfrak{a}}$ by assumption. That is $a^k \in \mathfrak{a}$ for some $k \in \mathbb{N}$ and hence $(a + \mathfrak{a})^k = a^k + \mathfrak{a} = 0 + \mathfrak{a}$ such that $a + \mathfrak{a}$ is a nilpotent of $R/\mathfrak{a}$.

- The equivalence (d) $\iff$ (e) is finally true by elementary logical operations (note that we may commute the quantifiers $\forall\, a$ and $\forall\, b$)

$$\begin{aligned}
\text{(d)} &\iff \forall\, a,b \in R \,:\, \neg\Big((ab \in \mathfrak{a}) \wedge (b \notin \mathfrak{a})\Big) \vee (a \in \sqrt{\mathfrak{a}}) \\
&\iff \forall\, a,b \in R \,:\, (ab \notin \mathfrak{a}) \vee (b \in \mathfrak{a}) \vee (a \in \sqrt{\mathfrak{a}}) \\
&\iff \forall\, b,a \in R \,:\, (ba \notin \mathfrak{a}) \vee (a \in \mathfrak{a}) \vee (b \in \sqrt{\mathfrak{a}}) \\
&\iff \forall\, a,b \in R \,:\, (ab \notin \mathfrak{a}) \vee (b \in \sqrt{\mathfrak{a}}) \vee (a \in \mathfrak{a}) \\
&\iff \forall\, a,b \in R \,:\, \neg\Big((ab \in \mathfrak{a}) \wedge (b \notin \sqrt{\mathfrak{a}})\Big) \vee (a \in \mathfrak{a}) \\
&\iff \text{(e)}
\end{aligned}$$

□

Proof of (2.90):
We will only prove statements (i) to (vii) here. Statement (viii) is concerned with localizations and requires the correspondence theorem of ideals in localizations. Its proof is hence postponed until we have shown this theorem. Hence it can be found on page (1102).

(i) If $\mathfrak{p} \trianglelefteq_{\mathfrak{i}} R$ is prime and we assume $ab \in \mathfrak{p}$ for some a, $b \in R$, then $a \notin \mathfrak{p}$ or $b \in \mathfrak{p}$. Thus if also $b \notin \mathfrak{p}$ then necessarily $a \in \mathfrak{p} \subseteq \sqrt{\mathfrak{p}}$. Thus $\mathfrak{p}$ is primary, by property (d) in (2.88).

(ii) Let $\mathfrak{p} := \sqrt{\mathfrak{a}}$, then $\mathfrak{p}$ is an ideal of R, due to (2.22.(ii)). Now assume $1 \in \mathfrak{p}$, then there would be some $k \in \mathbb{N}$ such that $1 = 1^k \in \mathfrak{a}$. That is $1 \in \mathfrak{a}$ and hence $\mathfrak{a} = R$ in contradiction to $\mathfrak{a}$ being a primary ideal. Now assume $ab \in \mathfrak{p}$ for some a, $b \in R$. That is there is some $k \in \mathbb{N}$ such that $(ab)^k = a^k b^k \in \mathfrak{a}$. If we have $b^k \in \sqrt{\mathfrak{a}} = \mathfrak{p}$ then $b \in \mathfrak{p}$, as $\mathfrak{p}$ is a radical ideal. Thus assume $b^k \notin \sqrt{\mathfrak{a}}$. Then by property (e) we get $a^k \in \mathfrak{a}$ and hence $a \in \mathfrak{p}$. Thus $\mathfrak{p}$ is a prime ideal.

(ii) It remains to prove that $\mathfrak{p} = \sqrt{\mathfrak{a}}$ is the uniquely determined minimal prime ideal containing $\mathfrak{a}$. Thus assume $\mathfrak{a} \subseteq \mathfrak{q} \trianglelefteq_{\mathfrak{i}} R$ is any prime ideal containing $\mathfrak{a}$. Then we have $\mathfrak{p} = \sqrt{\mathfrak{a}} \subseteq \sqrt{\mathfrak{q}} = \mathfrak{q}$. Thus if $\mathfrak{q} \subseteq \mathfrak{p}$, then $\mathfrak{p} = \mathfrak{q}$, such that $\mathfrak{p}$ is a minimal prime ideal containing $\mathfrak{a}$. And if $\mathfrak{p}_*$ is minimal then $\mathfrak{p} \subseteq \mathfrak{p}_*$ again and hence $\mathfrak{p}_* = \mathfrak{p}$, due to minimality. Thus $\mathfrak{p}$ also is uniquely determined.

(iii) Let $\mathfrak{m} := \sqrt{\mathfrak{a}}$ and assume that $\mathfrak{m}$ is maximal. Now consider any a, $b \in R$ such that $ab \in \mathfrak{a}$ but $b \notin \mathfrak{a}$. Then we have to prove $a \in \mathfrak{m}$ (in order to satisfy property (d) of primary ideals). Thus suppose $a \notin \mathfrak{m}$, then (because of the maximality of $\mathfrak{m}$) we had $R = \mathfrak{m} + aR$. That is there would be some $h \in R$ such that $1 - ah \in \mathfrak{m}$. And by definition of $\mathfrak{m}$ this is $(1-ah)^k \in \mathfrak{a}$ for some $k \in \mathbb{N}$. Now define

$$f \;:=\; -\sum_{i=1}^{k} (-1)^i \binom{k}{i} \frac{(ah)^i}{a} \;\in\; R$$

Then using the binomial rule we find $1 - af = (1-ah)^k \in \mathfrak{a}$ by a straightforward computation. That is $af + \mathfrak{a} = 1 + \mathfrak{a}$ and hence $0 + \mathfrak{a} = (f+\mathfrak{a})(0+\mathfrak{a}) = (f+\mathfrak{a})(ab+\mathfrak{a}) = (fa+\mathfrak{a})(b+\mathfrak{a}) = (1+\mathfrak{a})(b+\mathfrak{a}) = b + \mathfrak{a}$. That is $b \in \mathfrak{a}$ in contradiction to the assumption. Thus we have $a \in \mathfrak{m}$, which we had to prove.

(iv) From the assumption we get $\mathfrak{m} = \sqrt{\mathfrak{m}} = \sqrt{\mathfrak{m}^k} \subseteq \sqrt{\mathfrak{a}} \subseteq \sqrt{\mathfrak{m}} = \mathfrak{m}$ due to (2.22.(vi)) (and as any maximal ideal is prime and hence radical). Thus we have $\sqrt{\mathfrak{a}} = \mathfrak{m}$ and hence $\mathfrak{a}$ is a primary ideal by (iii).

(v) Denote $\mathfrak{a} := \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_k$, then we first note that according to (2.25.(v))

$$\sqrt{\mathfrak{a}} \;=\; \sqrt{\bigcap_{i=1}^{k} \mathfrak{a}_i} \;=\; \bigcap_{i=1}^{k} \sqrt{\mathfrak{a}_i} \;=\; \bigcap_{i=1}^{k} \mathfrak{p} \;=\; \mathfrak{p}$$

Now consider any $a, b \in R$ such that $b \notin \mathfrak{a}$. That is there is some $i \in 1 \ldots k$ such that $b \notin \mathfrak{a}_i$. But as $ab \in \mathfrak{a} \subseteq \mathfrak{a}_i$ and $\mathfrak{a}_i$ is primary we find $a \in \sqrt{\mathfrak{a}_i} = \mathfrak{p} = \sqrt{\mathfrak{a}}$. That is $\mathfrak{a}$ satisfies property (d) in (2.88).

(vi) Recall that $\mathfrak{a} : u = \{\, b \in R \mid bu \in \mathfrak{a} \,\}$. (1) Hence if $u \in \mathfrak{a}$ and $b \in R$, then $bu \in \mathfrak{a}$, too, since $\mathfrak{a}$ is an ideal. But this already means $b \in \mathfrak{a} : u$. (3) In this case we have $u \notin \mathfrak{p} = \sqrt{\mathfrak{a}}$. If $b \in \mathfrak{a} : u$ then $bu \in \mathfrak{a}$ and since $\mathfrak{a}$ is primary together these imply $b \in \mathfrak{a}$. Hence we have $\mathfrak{a} : u \subseteq \mathfrak{a}$. Conversely, if $b \in \mathfrak{a}$, then $bu \in \mathfrak{a}$ is trivial, as $\mathfrak{a}$ is an ideal and hence we have $b \in \mathfrak{a} : u$, such that $\mathfrak{a} \subseteq \mathfrak{a} : u$, as well. (2) We now have $u \notin \mathfrak{a}$. Consider any $b \in \sqrt{\mathfrak{a} : u}$, that is there is some $k \in \mathbb{N}$ such that $b^k u \in \mathfrak{a}$. As $u \notin \mathfrak{a}$ and $\mathfrak{a}$ is primary, we find $b^k \in \sqrt{\mathfrak{a}}$ and hence $b \in \sqrt{\mathfrak{a}} = \mathfrak{p}$, as $\sqrt{\mathfrak{a}}$ is a radical ideal. That is we have proved $\sqrt{\mathfrak{a} : u} \subseteq \mathfrak{p}$, but as $\mathfrak{a} \subseteq \mathfrak{a} : u$ the converse inclusion is clear from $\mathfrak{p} = \sqrt{\mathfrak{a}} \subseteq \sqrt{\mathfrak{a} : u}$. Thus we have $\sqrt{\mathfrak{a} : u} = \mathfrak{p}$. Now consider any $a, b \in R$ such that $ab \in \mathfrak{a} : u$ but $b \notin \mathfrak{a} : u$. This means $abu \in \mathfrak{a}$ but $bu \notin \mathfrak{a}$. As $\mathfrak{a}$ is primary we again find $a \in \sqrt{\mathfrak{a}} = \mathfrak{p} = \sqrt{\mathfrak{a} : u}$ and hence $\mathfrak{a} : u$ is primary, as well.

(vii) First observe that the radical of $\mathfrak{a}$ is truly given to be $\mathfrak{p}$, as we compute

$$\begin{aligned}
\sqrt{\mathfrak{a}} \;&=\; \left\{ a \in R \;\middle|\; \exists\, k \in \mathbb{N} \;:\; a^k \in \mathfrak{a} = \varphi^{-1}(\mathfrak{b}) \right\} \\
&=\; \left\{ a \in R \;\middle|\; \exists\, k \in \mathbb{N} \;:\; \varphi(a)^k = \varphi(a^k) \in \mathfrak{p} \right\} \\
&=\; \left\{ a \in R \;\middle|\; \exists\, \varphi(a) \in \sqrt{\mathfrak{b}} = \mathfrak{q} \right\} \;=\; \varphi^{-1}(\mathfrak{q}) \;=\; \mathfrak{p}
\end{aligned}$$

Thus consider $a, b \in R$ sucht that $ab \in \mathfrak{a}$ but $b \notin \mathfrak{a}$, that is $\varphi(a)\varphi(b) = \varphi(ab) \in \mathfrak{b}$ but $\varphi(b) \notin \mathfrak{b}$. As $\mathfrak{b}$ is primary this yields $\varphi(a) \in \sqrt{\mathfrak{b}} = \mathfrak{q}$ and hence $a \in \varphi^{-1}(\mathfrak{q}) = \sqrt{\mathfrak{a}}$. That is $\mathfrak{a}$ is primary again.

□

Proof of (2.91):

(i) Let us denote $\mathfrak{p} := pR$, then $\mathfrak{p}$ is a prime ideal, as p is a prime element. Also we have $\mathfrak{p}^n = p^n R = \mathfrak{a}$ and hence $\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{p}^n} = \sqrt{\mathfrak{p}} = \mathfrak{p}$. That is $\mathfrak{a}$ is associated to $\mathfrak{p}$. We will now prove, that $\mathfrak{a}$ is primary, by using induction on n. For $n = 1$ we have $\mathfrak{a} = pR = \mathfrak{p}$, that is $\mathfrak{a}$ is prime and hence primary by (2.90.(i)). Now consider any $n \geq 2$, and $a, b \in R$ such that $ab \in \mathfrak{a}$ but $b \notin \sqrt{\mathfrak{a}} = \mathfrak{p}$. That is there is some $h \in R$ such that $ab = p^n b$ but $p \not| b$. As p is prime, $p \mid hp^n = ab$ and $p \not| b$ we have $p \mid a$, that is there is some $\alpha \in R$ such that $a = \alpha p$. As R is an integral domain we get $\alpha b = (ab)/p = (p^n h)/p = p^{n-1} h$. Now from $ab \in p^{n-1}R$ and $b \notin \sqrt{p^{n-1}R} = \mathfrak{p}$ the induction hypothesis yields $\alpha \in p^{n-1}R$ and therefore $a = \alpha p \in p^n R = \mathfrak{a}$, that is $\mathfrak{a}$ is primary.

(ii) If $\mathfrak{a} = 0$ then $\mathfrak{a}$ is prime (as R is an integral domain) and hence primary (by (2.90.(i))). And if $\mathfrak{a} = p^n R$ for some prime element $p \in R$ and $1 \leq n \in \mathbb{N}$, then $\mathfrak{a}$ is primary, as we have seen in (i). Conversely consider any primary ideal $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$. As R is a PID it is generated by a single element

$\mathfrak{a} = aR$. Clearly $a \notin R^*$ (as else $\mathfrak{a} = R$ would not be primary). If $a = 0$ then $\mathfrak{a} = 0$ and hence there is nothing to prove. Thus assume $a \neq 0$, recall that R is an UFD by (2.79) and assume there would be two non-associate prime elements $p, q \in R$ such that $p \mid a$ and $q \mid a$. Then we let $m := \langle a \mid p \rangle$ and $n := \langle a \mid q \rangle$ (clearly $1 \leq m, n \in \mathbb{N}$ by (2.64.(iv))) and thereby get $p^m q^m \mid a$. That is there is some $b \in R$ such that $p^m q^n b = a$ and $p \nmid b$ and $q \nmid b$. It is clear that $p^m \notin \sqrt{\mathfrak{a}}$ as else there would be some $k \in \mathbb{N}$ such that $q \mid a \mid p^{mk}$. On the other hand we have $q^n b \notin \mathfrak{a}$, as else $p \mid a \mid q^n b$. This contradicts $\mathfrak{a}$ being a primary ideal and hence there is only one prime element $p \in R$ (up to associatedness) dividing a. Thus $a = \alpha p^m$ for some $\alpha \in R^*$ and this finally means $\mathfrak{a} = aR = p^n R$.

(iii) First of all $\mathfrak{m} = \langle s, t \rangle_{\mathrm{i}}$ is a maximal ideal, as $R/\mathfrak{m}$ is a field (in fact we find $R/\mathfrak{m} \cong_{\mathrm{r}} E : f + \mathfrak{m} \mapsto f(0,0)$). Further we have $\mathfrak{a} = \langle s, t^2 \rangle_{\mathrm{i}} \subseteq \langle s, t \rangle_{\mathrm{i}} = \mathfrak{m}$. It is even true that $t \notin \mathfrak{a}$ and hence $\mathfrak{a} \subset \mathfrak{m}$ (suppose $t = fs + gt^2$ for some $f, g \in R$. Then letting $t = 0$ we would find $0 = fs$ and hence $f = 0$. But this yields $1 = gt$ a contradiction to $t \notin R^*$). Next we have $\mathfrak{m} = \langle s^2, st, t^2 \rangle_{\mathrm{i}} \subseteq \langle s, t^2 \rangle_{\mathrm{i}} = \mathfrak{a}$. And in analogy to the above we find $s \notin \mathfrak{m}^2$, altogether this means

$$\mathfrak{m}^2 \subset \mathfrak{a} \subset \mathfrak{m}$$

As $\mathfrak{m}$ is maximal (2.90.(iv)) yields that $\mathfrak{a}$ is primary and associated to $\mathfrak{m}$. Now suppose there would be some $k \in \mathbb{N}$ and $\mathfrak{p} \in \operatorname{Spec}(R)$ such that $\mathfrak{a} = \mathfrak{p}^k$. Then from $\mathfrak{m}^2 \subseteq \mathfrak{a} = \mathfrak{p}^k \subseteq \mathfrak{m}$ we would get $\mathfrak{m} = \sqrt{\mathfrak{m}^2} \subseteq \mathfrak{p} = \sqrt{\mathfrak{p}^k} \subseteq \sqrt{\mathfrak{m}} = \mathfrak{m}$. That is $\mathfrak{p} = \mathfrak{m}$ and hence $\mathfrak{m}^2 \subset \mathfrak{a} = \mathfrak{m}^k \subset \mathfrak{m}$. If $k \leq 1$ then we have $\mathfrak{m}^k \supseteq \mathfrak{m}$ a contradiction. And if $k \geq 2$ then $\mathfrak{m}^2 \supseteq \mathfrak{m}^k$ a contradiction, too. Thus there is no prime ideal $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ and $k \in \mathbb{N}$ with $\mathfrak{a} = \mathfrak{p}^k$.

(iv) First of all it is clear that $\mathfrak{u} = \langle u^2 - st \rangle_{\mathrm{i}} \subseteq \langle t, u \rangle_{\mathrm{i}}$. And as $\langle t, u \rangle_{\mathrm{i}}$ is a prime ideal of $E[s,t,u]$ we find that $\mathfrak{p} = \langle t, u \rangle_{\mathrm{i}}/\mathfrak{u}$ is a prime ideal of R, due to the corresopndence theorem (1.66). Now regard

$$\mathfrak{a} = \langle b, c \rangle_{\mathrm{i}}^2 = \langle b^2, bc, c^2 \rangle_{\mathrm{i}} = \langle b^2, bc, ba \rangle_{\mathrm{i}} = (bR)\langle a, b, c \rangle_{\mathrm{i}}$$

Then it is clear that $\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{p}^2} = \mathfrak{p}$ and $ab = c^2 \in \mathfrak{a}$. However a (a bit cumbersome) computation yields $b \notin \mathfrak{a}$ and $a \notin \mathfrak{p} = \sqrt{\mathfrak{a}}$. This means that $\mathfrak{a}$ is not primary.

□

Proof of (2.92):

- As $\mathfrak{a} \neq R$ is a proper ideal, we have $1 \in R \setminus \mathfrak{a}$. Therefore for any $a \in \mathfrak{a}^n$ we have $a \cdot 1 \in \mathfrak{a}^n$ and thereby $a \in \mathfrak{a}^{(n)}$. This is $\mathfrak{a}^n \subseteq \mathfrak{a}^{(n)}$.

- Next we need to prove that $\mathfrak{p}^{(n)}$ truly is an ideal of R: As $0 \in \mathfrak{p}^n$ we already have $0 \in \mathfrak{p}^{(n)}$, too. Now consider any two $a, b \in \mathfrak{p}^{(n)}$, that is au and $bv \in \mathfrak{p}^n$ for some $u, v \in R \setminus \mathfrak{p}$. As $\mathfrak{p}$ is prime, we have $uv \in R \setminus \mathfrak{p}$ again. Yet also $(a+b)uv = (au)v + (bv)u \in \mathfrak{p}^n$ such that $a + b \in \mathfrak{p}^{(n)}$. Also for any $r \in R$ we get $(ra)u = r(au) \in \mathfrak{p}^n$ such that $ra \in \mathfrak{p}^{(n)}$, too. Altogether $\mathfrak{p}^{(n)}$ is an ideal of R.

- For (i) it only remains to prove $\mathfrak{p}^{(n)} \subseteq \mathfrak{p}$: So consider any $a \in \mathfrak{p}^{(n)}$, that is $au \in \mathfrak{p}^n$ for some $u \in R \setminus \mathfrak{p}$. As $au \in \mathfrak{p}^n \subseteq \mathfrak{p}$ and $\mathfrak{p}$ is prime we either have $a \in \mathfrak{p}$ or $u \in \mathfrak{p}$. But the latter is ruled out, so we are left with $a \in \mathfrak{p}$, which is $\mathfrak{p}^{(n)} \subseteq \mathfrak{p}$.

- Claim (ii) is immediate from the definition: As $\mathfrak{p}^{n+1} \subseteq \mathfrak{p}^n$ any $au \in \mathfrak{p}^{n+1}$ is already contained in $au \in \mathfrak{p}^n$. Therefore $a \in \mathfrak{p}^{(n+1)}$ implies $a \in \mathfrak{p}^{(n)}$.

- From this we can easily conclude $\sqrt{\mathfrak{p}^{(n)}} = \mathfrak{p}$: By (2.25.(vi)) and (i) we get the chain of inclusions $\mathfrak{p} = \sqrt{\mathfrak{p}^n} \subseteq \sqrt{\mathfrak{p}^{(n)}} \subseteq \sqrt{\mathfrak{p}} = \mathfrak{p}$. Hence, as the radical of $\mathfrak{p}^{(n)}$ is constrained by $\mathfrak{p}$ from both sides, it has to be equal to $\mathfrak{p}$.

- To conclude (iii) we have to prove, that $\mathfrak{p}^{(n)}$ is a primary ideal: That is we start with $ab \in \mathfrak{p}^{(n)}$ such that $b \notin \sqrt{\mathfrak{p}^{(n)}} = \mathfrak{p}$. That is there is some $u \notin \mathfrak{p}$ such that $abu \in \mathfrak{p}^n$. But as both b, $u \notin \mathfrak{p}$ and $\mathfrak{p}$ is prime, we again conclude $bu \notin \mathfrak{p}$. But $a(bu) \in \mathfrak{p}^n$ is precisely what it takes for $a \in \mathfrak{p}^{(n)}$, such that $\mathfrak{p}^{(n)}$ is primary, by property (e).

- It remains to verify (iv): As $\mathfrak{p}^n \subseteq \mathfrak{p}^{(n)}$ we already have $\mathfrak{p}^n R_{\mathfrak{p}} \subseteq \mathfrak{p}^{(n)} R_{\mathfrak{p}}$. Conversely we start with $a/u \in \mathfrak{p}^{(n)} R_{\mathfrak{p}}$ that is $av \in \mathfrak{p}^n$ for some $v \in R \setminus \mathfrak{p}$. However this already is $a/u = (av)/(uv) \in \mathfrak{p}^n R_{\mathfrak{p}}$ such that $\mathfrak{p}^{(n)} R_{\mathfrak{p}} \subseteq \mathfrak{p}^n R_{\mathfrak{p}}$, too.

□

Proof of (2.94):

(i) Suppose $\mathfrak{p} = \mathfrak{a} \cap \mathfrak{b}$ for some ideals $\mathfrak{a}$, $\mathfrak{b} \trianglelefteq_{\mathrm{i}} R$ with $\mathfrak{a} \neq \mathfrak{p}$ and $\mathfrak{p} \neq \mathfrak{b}$. As $\mathfrak{p} = \mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a}$ this means $\mathfrak{p} \subset \mathfrak{a}$, that is there is some $a \in \mathfrak{a}$ with $a \notin \mathfrak{p}$. Likewise there is some $b \in \mathfrak{b}$ with $b \notin \mathfrak{p}$. Yet $ab \in \mathfrak{a} \cap \mathfrak{b} = \mathfrak{p}$, and as $\mathfrak{p}$ is prime this yields $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, a contradiction. Thus there are no such $\mathfrak{a}$, $\mathfrak{b}$ and this means that $\mathfrak{p}$ is irreducible.

(ii) Consider a, $b \in R$ such that $ab \in \mathfrak{p}$ but $b \notin \mathfrak{p}$. We will prove $a \in \sqrt{\mathfrak{p}}$ which is property (d) of primary ideals. Thus let $\mathfrak{b} := \mathfrak{p} + bR$. Then we regard the following ascending chain of ideals

$$\mathfrak{p} \subseteq \mathfrak{p} : a \subseteq \mathfrak{p} : a^2 \subseteq \ldots \subseteq \mathfrak{p} : a^k \subseteq \mathfrak{p} : a^{k+1} \subseteq \ldots$$

As R is noetherian this chain has to stabilize. That is there is some $s \in \mathbb{N}$ such that for all $i \in \mathbb{N}$ we get $\mathfrak{p} : a^s = \mathfrak{p} : a^{s+i}$. Now let $\mathfrak{a} := \mathfrak{p} + a^s R$. Then we will prove

$$\mathfrak{p} = \mathfrak{a} \cap \mathfrak{b}$$

The inclusion "$\subseteq$" is clear, as $\mathfrak{p} \subseteq \mathfrak{a}$ and $\mathfrak{p} \subseteq \mathfrak{b}$ by construction. Thus consider any $h \in \mathfrak{a} \cap \mathfrak{b}$. As $h \in \mathfrak{b} = \mathfrak{p} + bR$ there are some $q \in \mathfrak{p}$ and $g \in R$ such that $h = q + bg$. Therefore $ah = aq + abg \in \mathfrak{p}$ as we have $ab \in \mathfrak{p}$. And as $h \in \mathfrak{a} = \mathfrak{p} + a^s R$ as well, there are some $p \in \mathfrak{p}$ and $f \in R$ such that $h = p + a^s f$. Hence $ah = ap + a^{s+1} f$ such that $a^{s+1} f = ah - ap$. Now recall that $ah \in \mathfrak{p}$, then $a^{s+1} f = ah - ap \in \mathfrak{p}$ and this means $f \in \mathfrak{p} : a^{s+1} = \mathfrak{p} : a^s$. Therefore we have $a^s f \in \mathfrak{p}$ and this finally means $h = p + a^s f \in \mathfrak{p}$. Thus we have established $\mathfrak{p} = \mathfrak{a} \cap \mathfrak{b}$. However as $b \notin \mathfrak{p}$ we have $\mathfrak{p} \subset \mathfrak{b}$. And hence the irreducibility of $\mathfrak{p}$ yields $\mathfrak{p} = \mathfrak{a} = \mathfrak{p} + a^s R$. In particular $a^s \in \mathfrak{p}$ and that is $a \in \sqrt{\mathfrak{p}}$ which had to be shown.

(iii) Let us denote the set of all proper ideals that do *not* satisfy the claim (i.e. that are *no* finite intersection of irreducible ideals) by

$$\mathcal{A} := \{ \mathfrak{a} \trianglelefteq_{\mathrm{i}} R \mid \mathfrak{a} \neq R,\ \nexists \mathfrak{p}_1, \ldots, \mathfrak{p}_k \trianglelefteq_{\mathrm{i}} R : \text{(1) and (2)} \}$$

We have to prove $\mathcal{A} = \emptyset$, thus assume $\mathcal{A} \neq \emptyset$, as R is a noetherian ring this would mean that $\mathcal{A}$ contains a maximal element $\mathfrak{a}^* \in \mathcal{A}^*$. As $\mathfrak{a}^* \in \mathcal{A}$ we in particular have that $\mathfrak{a}^*$ is not irreducible (else $\mathfrak{a}^*$ would be its own irreducible decomposition). And as also $\mathfrak{a}^* \neq R$ this means that there are ideals $\mathfrak{a}$, $\mathfrak{b} \trianglelefteq_{\mathrm{i}} R$ such that $\mathfrak{a}^* = \mathfrak{a} \cap \mathfrak{b}$ and $\mathfrak{a}^* \subset \mathfrak{a}$ and $\mathfrak{a}^* \subset \mathfrak{b}$. By maximality of $\mathfrak{a}^*$ this means $\mathfrak{a}, \mathfrak{b} \notin \mathcal{A}$ and hence there are irreducible decompositions $(\mathfrak{p}_1, \ldots, \mathfrak{p}_k)$ of $\mathfrak{a}$ and $(\mathfrak{q}_1, \ldots, \mathfrak{q}_l)$ of $\mathfrak{b}$. Hence

$$\mathfrak{a}^* \;=\; \mathfrak{a} \cap \mathfrak{b} \;=\; \left(\bigcap_{i=1}^{k} \mathfrak{p}_i\right) \cap \left(\bigcap_{j=1}^{l} \mathfrak{q}_i\right)$$

This means that $\mathfrak{a}^*$ admits $(\mathfrak{p}_1, \ldots, \mathfrak{p}_k, \mathfrak{q}_1, \ldots, \mathfrak{q}_l)$ as an irreducible decomposition and hence $\mathfrak{a}^* \notin \mathcal{A}$, a contradiction. Thus we have $\mathcal{A} = \emptyset$, that is *every* proper ideal of R admits an irreducible decomposition.

□

Proof of (2.98):
By assumption (2) we have $\mathfrak{a}_N = \mathfrak{a}$ for $N := 1 \ldots n$. And hence we may choose a subset M of minimal cardinality with this property. So step (1) of the proposition is legitimate. Now it is clear that $\approx$ is an equivalence relation on M, as it belongs to the function

$$p \;:\; M \to \operatorname{Spec}(R) \;:\; i \mapsto \sqrt{\mathfrak{a}_i}$$

Hence $A = M/\approx$ is a well defined partition of M (the equivalence classes $\alpha \in A$ are just the fibers of p). And for any $\alpha = [i] \in A$ we may define $\mathfrak{p}_\alpha := \sqrt{\mathfrak{a}_i}$. That is for any $\alpha \in A$ the set $\{\mathfrak{a}_i \mid i \in \alpha\}$ is a finite collection of primary ideals associated to $\mathfrak{p}_\alpha$. Hence by (2.90.(v)) $\mathfrak{a}_\alpha$ is a primary ideal associated to $\mathfrak{p}_\alpha$ as well. In particular $(\mathfrak{a}_\alpha)$ (where $\alpha \in A$) satisfies property (1) of primary decompositions. Further we have

$$\bigcap_{\alpha \in A} \mathfrak{a}_\alpha \;=\; \bigcap_{\alpha \in A} \bigcap_{i \in \alpha} \mathfrak{a}_i \;=\; \bigcap_{i \in M} \mathfrak{a}_i \;=\; \mathfrak{a}$$

as the α partition M and construction of M. Thus also property (2) of primary decompositions is satisfied. And property (4) is clear from the construction of A precisely by this relation. It remains to verify property (3). That is fix any $\beta = [j] \in A$ and assume $\mathfrak{a} = \bigcap_{\alpha \neq \beta} \mathfrak{a}_\alpha$. As $j \in \beta$ we in particular find

$$\mathfrak{a} \;=\; \bigcap_{i \in M} \mathfrak{a}_i \;\subseteq\; \bigcap_{j \neq i \in I} \mathfrak{a}_i \;\subseteq\; \bigcap_{\beta \neq \alpha \in A} \mathfrak{a}_\alpha \;=\; \mathfrak{a}$$

But this would mean $\mathfrak{a} = \bigcap_{i \neq j} \mathfrak{a}_i$ in contradiction to the minimality of M. Altogether we have proved properties (1) to (4), that is $(\mathfrak{a}_\alpha)$ (where $\alpha \in A$) is a minimal primary decomposition of $\mathfrak{a}$. □

Proof of (2.99):

(i) By definition $\#\mathrm{ass}(\mathfrak{a}_1, \ldots, \mathfrak{a}_k) = \#\{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\} \leq k$. And if we suppose $\mathfrak{p}_i = \mathfrak{p}_j$ then by minimality of $(\mathfrak{a}_1, \ldots, \mathfrak{a}_k)$ we have $i = j$ (this is property (4)). Hence we even find $\#\{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\} = k$ as claimed.

(ii) As $\mathfrak{a} = \bigcap_i \mathfrak{a}_i$ and using (2.22.(vi)) and (2.25.(v)) we can easily compute

$$\sqrt{\mathfrak{a} : u} \;=\; \sqrt{\left(\bigcap_{i=1}^{k} \mathfrak{a}_i\right) : u} \;=\; \sqrt{\bigcap_{i=1}^{k} (\mathfrak{a}_i : u)} \;=\; \bigcap_{i=1}^{k} \sqrt{\mathfrak{a}_i : u}$$

If $u \in \mathfrak{a}_i$ then we have $\mathfrak{a}_i : u = R$ according to (2.22.(iv)). And if $u \notin \mathfrak{a}_i$ then $\mathfrak{a}_i : u$ is primary again with $\sqrt{\mathfrak{a}_i : u} = \sqrt{\mathfrak{a}_i} = \mathfrak{p}_i$ by virtue of (2.90.(vi)). Thus we have obtained

$$\sqrt{\mathfrak{a} : u} \;=\; \bigcap_{i=1}^{k} \begin{cases} R \text{ if } u \in \mathfrak{a}_i \\ \mathfrak{p}_i \text{ if } u \notin \mathfrak{a}_i \end{cases}$$

Thus we may ignore any $i \in 1 \ldots k$ with $u \in \mathfrak{a}_i$, as they do not contribute to the intersection. What remains is precisely the claim

$$\sqrt{\mathfrak{a} : u} \;=\; \bigcap_{u \notin \mathfrak{a}_i} \mathfrak{p}_i$$

(iv) If $\mathfrak{p} \in \operatorname{ass}(\mathfrak{a})$ then by definition of $\operatorname{ass}(\mathfrak{a})$ there is some $u \in R$ such that $\mathfrak{p} = \sqrt{\mathfrak{a} : u}$. Thus by (ii) we have the identity

$$\mathfrak{p} \;=\; \bigcap_{u \notin \mathfrak{a}_i} \mathfrak{p}_i$$

And hence by (2.14.(ii)) there is some $i \in 1 \ldots k$ satisfying ($u \notin \mathfrak{a}_i$ and) $\mathfrak{p}_i \subseteq \mathfrak{p}$. And as $\mathfrak{p} \subseteq \mathfrak{p}_i$ is clear this is $\mathfrak{p} = \mathfrak{p}_i \in \operatorname{ass}(\mathfrak{a}_1, \ldots, \mathfrak{a}_k)$. Conversely choose any $j \in 1 \ldots k$. As $(\mathfrak{a}_1, \ldots, \mathfrak{a}_k)$ is minimal we have $\mathfrak{a} \subset \bigcap_{i \neq j} \mathfrak{a}_i$ and hence there is some $u_i \in \mathfrak{a}_i$ for any $i \neq j$ but $u_j \notin \mathfrak{u}_j$. Thus for this u_j by (ii) we get

$$\bigcap_{u_j \notin \mathfrak{a}_i} \mathfrak{p}_i \;=\; \mathfrak{p}_j \;=\; \sqrt{\mathfrak{a} : u_j} \;\in\; \operatorname{ass}(\mathfrak{a})$$

(iii) Without loss of generality we consider $\mathfrak{p}_1 \in \operatorname{ass}(\mathfrak{a}_1, \ldots, \mathfrak{a}_k)_*$. That is for any $i \in 2 \ldots k$ we have $\mathfrak{p}_i \not\subseteq \mathfrak{p}_1$. And this again means that there is some $a \in \mathfrak{p}_i$ with $a \notin \mathfrak{p}_1$. Now let $U := R \setminus \mathfrak{p}_1$, in particular $a \in U$. Then because of $a \in \mathfrak{p}_i = \sqrt{\mathfrak{a}_i}$ there is some $n \in \mathbb{N}$ such that $a^n \in \mathfrak{a}_i$. And as $a^n \in U$, too, we get $1/1 = (a^n)/(a^n) \in U^{-1}\mathfrak{a}_i$. Hence we get $U^{-1}\mathfrak{a}_i = U^{-1}R$ and this again means

$$R \;=\; \left(U^{-1}\mathfrak{a}_i\right) \cap R \;=\; \mathfrak{a}_i : U$$

for any $i \in 2 \ldots k$. This now can be used to prove $\mathfrak{a} : U = \mathfrak{a}_1$ by virtue of the following computation (see (2.125) - for convenience we even gave an elementary proof of $(\mathfrak{a} \cap \mathfrak{b}) : U = (\mathfrak{a} : U) \cap (\mathfrak{b} : U)$ there)

$$\mathfrak{a} : U \;=\; \left(\bigcap_{i=1}^{k} \mathfrak{a}_i\right) : U \;=\; \bigcap_{i=1}^{k} (\mathfrak{a}_i : U) \;=\; \mathfrak{a}_1 : U \;=\; \mathfrak{a}_1$$

Hereby $\mathfrak{a}_1 : U = \mathfrak{a}_1$ holds true because $\mathfrak{a}_1$ is primary and $U = R \setminus \mathfrak{p}_1$. To be precise consider $a \in \mathfrak{a}_i : U$, that is there is some $u \in U$ such that $au \in \mathfrak{a}_i$. But by definition of U we have $u \notin \mathfrak{p}_1 = \sqrt{\mathfrak{a}_1}$, and as $\mathfrak{a}_1$ is primary this yields $a \in \mathfrak{a}_1$. Thus we have $\mathfrak{a}_1 : U \subseteq \mathfrak{a}_1$ and the converse inclusion is trivial.

(v) If $\mathfrak{p} \in \operatorname{ass}(\mathfrak{a})_*$ then by virtue of (iv) we have $\mathfrak{p} = \mathfrak{p}_i$ for some $i \in 1 \ldots k$. And as $\mathfrak{p}_i$ is minimal (iii) implies $\mathfrak{a} : (R \setminus \mathfrak{p}) = \mathfrak{a}_i \in \operatorname{iso}(\mathfrak{a}_1, \ldots, \mathfrak{a}_k)$. Conversely consider any $\mathfrak{a}_i \in \operatorname{iso}(\mathfrak{a}_1, \ldots, \mathfrak{a}_k)$. Then by

definition $\mathfrak{p}_i \in \operatorname{ass}(\mathfrak{a}_1,\ldots,\mathfrak{a}_k)_*$ and by (iii) this means $\mathfrak{a}_i = \mathfrak{a} : (R \setminus \mathfrak{p})$. And by (iv) we also have $\mathfrak{p}_i \in \operatorname{ass}(\mathfrak{a})_*$ and thereby $\mathfrak{a}_i \in \operatorname{iso}(\mathfrak{a})$.

□

Proof of (2.101):

(1) By (2.94.(iii)) there are some irreducible ideals $\mathfrak{p}_1,\ldots,\mathfrak{p}_k \trianglelefteq_{\mathrm{i}} R$ such that $\mathfrak{a} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_k$. And by (2.94.(ii)) these irreducible ideals already are primary. Thus $(\mathfrak{p}_1,\ldots,\mathfrak{p}_k)$ is a primary decomposition of $\mathfrak{a}$. And by (2.98) we find that $\mathfrak{a}$ then already has a minimal primary decomposition.

(2) Now assume that $(\mathfrak{a}_1,\ldots,\mathfrak{a}_k)$ and $(\mathfrak{b}_1,\ldots,\mathfrak{b}_l)$ are minimal primary decompositions of $\mathfrak{a}$. Then by (2.99.(iii)) we get the identity

$$\operatorname{ass}(\mathfrak{a}_1,\ldots,\mathfrak{a}_k) \;=\; \operatorname{ass}(\mathfrak{a}) \;=\; \operatorname{ass}(\mathfrak{b}_1,\ldots,\mathfrak{b}_l)$$

(Note that by definition $\operatorname{ass}(\mathfrak{a})$ and $\operatorname{iso}(\mathfrak{a})$ only depend on $\mathfrak{a}$, not on the decomposition). And by (2.99.(i)) this in particular implies $k = l$. The third identity we finally get from (2.99.(iv))

$$\operatorname{iso}(\mathfrak{a}_1,\ldots,\mathfrak{a}_k) \;=\; \operatorname{iso}(\mathfrak{a}) \;=\; \operatorname{iso}(\mathfrak{b}_1,\ldots,\mathfrak{b}_l)$$

(3) Let us denote the minimal prime ideals over $\mathfrak{a}$ by $\mathfrak{a}_i$, that is we let $\{\mathfrak{a}_1,\ldots,\mathfrak{a}_k\} := \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{a} \subseteq \mathfrak{p}\}_*$ (note that there are only finitely many $\mathfrak{a}_i$, due to (2.45.(iii))). Then by (2.25.(i)) we have

$$\mathfrak{a} \;=\; \sqrt{\mathfrak{a}} \;=\; \bigcap \{\,\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{a} \subseteq \mathfrak{p}\,\}_* \;=\; \bigcap_{i=1}^{k} \mathfrak{a}_i$$

And as the $\mathfrak{a}_i$ are prime they in particular are primary according to (2.94.(i)). That is $(\mathfrak{a}_1,\ldots,\mathfrak{a}_k)$ is a primary decomposition of $\mathfrak{a}$. And as $\sqrt{\mathfrak{a}_i} = \mathfrak{a}_i \neq \mathfrak{a}_j = \sqrt{\mathfrak{a}_j}$ (for $i \neq j$) it even satisfies property (4) of minimal primary decompositions. Now assume that for some index $j \in 1\ldots k$ we had the equality

$$\bigcap_{i \neq j} \mathfrak{a}_i \;=\; \mathfrak{a} \;\subseteq\; \mathfrak{a}_j$$

Then by (2.14.(ii)) there would be some $i \neq j$ such that $\mathfrak{a} \subseteq \mathfrak{a}_i \subseteq \mathfrak{a}_j$. And by minimality of $\mathfrak{a}_j$ this would mean $\mathfrak{a}_i = \mathfrak{a}_j$, a contradiction. Thus $(\mathfrak{a}_1,\ldots,\mathfrak{a}_k)$ also satisfies property (3), that is it *is* a minimal primary decomposition of $\mathfrak{a}$. In fact this even is $\operatorname{ass}(\mathfrak{a}_1,\ldots,\mathfrak{a}_k) = \operatorname{iso}(\mathfrak{a}_1,\ldots,\mathfrak{a}_k)$, that is every associated ideal is an isolated component. Now assume that $(\mathfrak{b}_1,\ldots,\mathfrak{b}_l)$ is any minimal primary decomposition of $\mathfrak{a}$, then by (2) we have $l = k$ and

$$\begin{aligned} \{\,\mathfrak{a}_1,\ldots,\mathfrak{a}_k\,\} &= \operatorname{ass}(\mathfrak{a}_1,\ldots,\mathfrak{a}_k) \\ &= \operatorname{iso}(\mathfrak{a}_1,\ldots,\mathfrak{a}_k) \\ &= \operatorname{iso}(\mathfrak{b}_1,\ldots,\mathfrak{b}_k) \end{aligned}$$

That is for any $i \in 1\ldots k$ we have $\mathfrak{a}_i \in \operatorname{iso}(\mathfrak{b}_1,\ldots,\mathfrak{b}_k) = \{\,\mathfrak{a}_1,\ldots,\mathfrak{a}_k\,\}$ and this again means that for any $i \in 1\ldots k$ there is some $\sigma(i) \in 1\ldots k$ such that $\mathfrak{b}_i = \mathfrak{a}_{\sigma(i)}$. Clearly σ is injective, because if we assume $\sigma(i) = \sigma(j)$ then $\mathfrak{b}_i = \mathfrak{a}_{\sigma(i)} = \mathfrak{a}_{\sigma(j)} = \mathfrak{b}_j$ in contradiction to the minimality

of $(\mathfrak{b}_1,\ldots,\mathfrak{b}_k)$. But as k is finite this already means that σ is bijective, that is $\sigma \in S_k$. Altogether $(\mathfrak{b}_1,\ldots,\mathfrak{b}_k)$ is just a rearranged version of $(\mathfrak{a}_1,\ldots,\mathfrak{a}_k)$.

□

Proof of (2.102):

(i) Let $(\mathfrak{a}_1,\ldots,\mathfrak{a}_k)$ be a minimal primary decomposition of $\mathfrak{a}$ (which exists, due to (2.101)) and $\mathfrak{p}_i := \sqrt{\mathfrak{a}_i}$. Then we have seen in (2.99.(iv)) that $\operatorname{ass}(\mathfrak{a}) = \{\mathfrak{p}_1,\ldots,\mathfrak{p}_k\}$. Thus from $\bigcap_i \mathfrak{a}_i = \mathfrak{a} \subseteq \mathfrak{q}$ we get $\mathfrak{a}_i \subseteq \mathfrak{q}$ for some $i \in 1\ldots k$, according to (2.14.(ii)). Therefore $\mathfrak{p}_i = \sqrt{\mathfrak{a}_i} \subseteq \sqrt{\mathfrak{q}} = \mathfrak{q}$ and $\mathfrak{p}_i \in \operatorname{ass}(\mathfrak{a})$. Now let $\mathfrak{p}_j \subseteq \mathfrak{q}$ for some $\mathfrak{p}_j \in \operatorname{ass}(\mathfrak{a})$. Then we may choose some minimal $\mathfrak{p}_i \in \operatorname{ass}(\mathfrak{a})_*$ with $\mathfrak{p}_i \subseteq \mathfrak{p}_j$ (as $\operatorname{ass}(\mathfrak{a})$ is finite). And hence we get $\mathfrak{a}_i \subseteq \mathfrak{p}_i \subseteq \mathfrak{p}_j \subseteq \mathfrak{q}$, that is $\mathfrak{a}_i \subseteq \mathfrak{q}$. Finally consider $\mathfrak{a}_i \subseteq \mathfrak{q}$ then $\mathfrak{a} \subseteq \mathfrak{a}_i \subseteq \mathfrak{q}$ is clear.

(ii) We stick to the notation used for (i) that is $(\mathfrak{a}_1,\ldots,\mathfrak{a}_k)$ is a minimal primary decomposition and $\mathfrak{p}_i := \sqrt{\mathfrak{a}_i}$. "$\subseteq$" if $\mathfrak{a} \subseteq \mathfrak{q}$ then by (i) there exists some $\mathfrak{a}_i \in \operatorname{iso}(\mathfrak{a})$ such that $\mathfrak{a}_i \subseteq \mathfrak{q}$. Then $\mathfrak{a} \subseteq \mathfrak{a}_i \subseteq \mathfrak{p}_i = \sqrt{\mathfrak{a}_i} \subseteq \sqrt{\mathfrak{q}} = \mathfrak{q}$. By minimality of $\mathfrak{q}$ this yields $\mathfrak{q} = \mathfrak{p}_i \in \operatorname{ass}(\mathfrak{a})_*$. "$\supseteq$" conversely, if $\mathfrak{p}_i \in \operatorname{ass}_*$ then $\mathfrak{a} \subseteq \mathfrak{a}_i \subseteq \mathfrak{p}_i$. Thus if we consider any prime ideal $\mathfrak{p} \trianglelefteq_{\mathfrak{i}} R$ such that $\mathfrak{a} \subseteq \mathfrak{p} \subseteq \mathfrak{p}_i$, then by (i) there is some $\mathfrak{p}_j \in \operatorname{ass}(\mathfrak{a})$ such that $\mathfrak{p}_j \subseteq \mathfrak{p} \subseteq \mathfrak{p}_i$. By minimality of $\mathfrak{p}_i$ in $\operatorname{ass}(\mathfrak{a})$ this means $\mathfrak{p}_j = \mathfrak{p}_i$ and hence $\mathfrak{p} = \mathfrak{p}_i$. Hence $\mathfrak{p}_i$ is a minimal prime ideal containing $\mathfrak{a}$.

(iii) This follows immediately from (ii) and (2.25.(i)): by the propositions cited, we have $\sqrt{\mathfrak{a}} = \bigcap\{\mathfrak{q} \in \operatorname{Spec}(R) \mid \mathfrak{a} \subseteq \mathfrak{q}\} = \bigcap \operatorname{ass}(\mathfrak{a})_*$. And it is clear that $\bigcap \operatorname{ass}(\mathfrak{a}) \subseteq \bigcap \operatorname{ass}(\mathfrak{a})_*$, as $\operatorname{ass}(\mathfrak{a})_* \subseteq \operatorname{ass}(\mathfrak{a})$. But on the other hand, if $\mathfrak{i} \in \operatorname{ass}(\mathfrak{a})$ there some $\mathfrak{i}_* \in \operatorname{ass}(\mathfrak{a})_*$ such that $\mathfrak{i}_* \subseteq \mathfrak{i}$ (as $\operatorname{ass}(\mathfrak{a})$ is finite). Thus we also have $\bigcap \operatorname{ass}(\mathfrak{a})_* \subseteq \bigcap \operatorname{ass}(\mathfrak{a})$.

□

Proof of (2.105):

We will first prove the ζ truly is a homomorphism of rings. By definition we have $\zeta(0) = 0_R$ and $\zeta(1) = 1_R$. If now $k \in \mathbb{N}$ then $\zeta(-k) = k(-1_R) = -(k1_R) = -\zeta(k)$ by general distributivity. Hence we have $\zeta(-k) = -\zeta(k)$ *for any* $k \in \mathbb{Z}$ (because if $k < 0$ then $-k \in \mathbb{N}$ and hence $-\zeta(k) = -\zeta(--k) = --\zeta(-k) = \zeta(-k)$). This will be used to prove the additivity of ζ. First of all it is clear that for i, $j \in \mathbb{N}$ we get

$$\zeta(i+j) \;=\; (i+j)1_R \;=\; (i1_R) + (j1_R) \;=\; \zeta(i) + \zeta(j)$$

And likewise $\zeta((-i)+(-j)) = \zeta(-(i+j)) = -\zeta(i+j) = -(\zeta(i)+\zeta(j)) = -\zeta(i) + -\zeta(j) = \zeta(-i) + \zeta(-j)$. Now assume $i \geq j$ then by general associativity it is clear that $\zeta(i+(-j)) = \zeta(i-j) = (i-j)1_R = (i1_R) - (j1_R) = \zeta(i) - \zeta(j) = \zeta(i) + \zeta(-j)$. And if $i \leq j$ then $\zeta(i+(-j)) = \zeta(-(j-i)) = -\zeta(j-i) = -\zeta(j) + \zeta(-i) = \zeta(-j) + -\zeta(-i) = \zeta(i) + \zeta(-j)$. Thus in any case we have $\zeta(i+(-j)) = \zeta(i)+\zeta(-j)$ and likewise we see $\zeta((-i)+j) = \zeta(-i)+\zeta(j)$. Thus we have finally arrived at $\zeta(i+j) = \zeta(i)+\zeta(j)$ for any i, $j \in \mathbb{Z}$. For the multiplicativity things are considerably simpler: let i, $j \in \mathbb{N}$ again, then by the general rule of distributivity we get $\zeta(ij) = (ij)1_R = (i1_R)(j1_R) = \zeta(i)\zeta(j)$. And as also $\zeta(-k) = -\zeta(k)$ this clearly yields $\zeta(ij) = \zeta(i)\zeta(j)$ for any i, $j \in \mathbb{Z}$. Thus ζ is a homomorphism of rings. And if $\varphi : \mathbb{Z} \to R$ is any homomorphism, then $\varphi(1) = 1_R$. By induction on $k \in \mathbb{N}$ we see $\varphi(k) = \varphi(1+\cdots+1) = \varphi(1)+\cdots+\varphi(1) = 1_R+\cdots+1_R = k1_R = \zeta(k)$. And of course $\varphi(-k) = -\varphi(k) = -\zeta(k) = \zeta(-k)$ such that $\varphi = \zeta$. This also is the uniqueness of ζ.

Thus $\mathrm{im}(\zeta)$ is a sub-ring of R by virtue of (1.76.(v)). Let us denote the intersection of all sub-rings of R by P - note that this is a sub-ring again, due to (1.52). From the construction of P it is clear, that $P \subseteq \mathrm{im}(\zeta) \leq_\mathrm{r} R$. But as $1_R \in P$ we have and hence $\zeta(k) = k1_R \in P$ f0r any $k \in \mathbb{N}$. Likewise $-1_R \in P$ and hence $\zeta(-k) = k(-1_R) \in P$. This is the converse inclusion $\mathrm{im}(\zeta) \subseteq P$ and hence $\mathrm{im}(\zeta) = P$.
Now $\mathrm{kn}(\zeta) \trianglelefteq_\mathrm{i} \mathbb{Z}$ is an ideal in $\mathbb{Z}$ due to (1.76.(v)) again. But as $(\mathbb{Z}, \alpha)$ is an Euclidean domain $\mathbb{Z}$ is a PID due to (2.79.(iii)). Hence there is some $n \in \mathbb{Z}$ such that $\mathrm{kn}(\zeta) = n\mathbb{Z}$. Thereby n is determined up to associatedness. And as $\mathbb{Z}^* = \{1, -1\}$ this is n is uniquely determined up to sign $\pm n$. Thus by fixing $n \geq 0$ it is uniquely determined. Now

$$\begin{aligned}\mathrm{kn}(\zeta) &= \{\, k \in \mathbb{Z} \mid \zeta(k) = 0_R \,\} \\ &= \{\, \pm k \mid k \in \mathbb{N},\ \zeta(k) = 0_R \,\} \\ &= \{\, \pm k \mid k \in \mathbb{N},\ k1_R = 0_R \,\}\end{aligned}$$

Thus if $n = 0$ then $\mathrm{kn}(\zeta) = 0$ and hence $k1_R = 0_R$ implies $k \in \mathrm{kn}(\zeta) = 0$ which is $k = 0$. And if $n \neq 0$ then $\mathrm{kn}(\zeta) \neq 0$. And hence we have seen in (2.79.(iii)) that $\alpha(n) = |n| = n$ is minimal in $\mathrm{kn}(\zeta)$. And due to the explict realisation of the kernel above this is $n = \min\{\, 1 \leq k \in \mathbb{N} \mid k1_R = 0 \,\}$. □

Proof of (2.107):

(i) As R is an integral domain, so are its sub-rings $P \leq_\mathrm{r} R$. In particular $\mathrm{im}(\zeta) \leq_\mathrm{r} R$ is an integral domain. But by definition and (1.83.(ii)) we've got the isomorphy (where $n := \mathrm{CHAR}(R)$)

$$\mathbb{Z}\big/_{n\mathbb{Z}} = \mathbb{Z}\big/_{\mathrm{kn}(\zeta)} \cong_\mathrm{r} \mathrm{im}(\zeta) = \mathrm{PRR}(R) \leq_\mathrm{r} R$$

Hence $\mathbb{Z}/n\mathbb{Z}$ is an integral domain, too and by (2.12) this implies that $n\mathbb{Z} = \mathbb{Z}$ or $n\mathbb{Z}$ is a prime ideal in $\mathbb{Z}$. If we had $n\mathbb{Z} = \mathbb{Z}$, then $n = 1$, which would mean $1_R = 0_R$ in contradiction to $R \neq 0$. This only leaves, that $n\mathbb{Z}$ is a prime ideal. But this again means that $n = 0$ or that n is prime because of (2.58.(ii)).

(ii) Suppose $n := \mathrm{CHAR}(R) = 0$ and $k_R = 0_R$, then $k \in \mathrm{kn}(\zeta) = n\mathbb{Z} = 0$ which is $k = 0$. Conversely suppose $n \in n\mathbb{Z} = \mathrm{kn}(\zeta)$, that is $n_R = \zeta(n) = 0_R$ and by assumption this implies $n = 0$. We now prove the second equivalence. That is we assume $n = 0$ and want to show $\zeta : \mathbb{Z} \cong_\mathrm{r} \mathrm{PRR}(R)$. But as in (i) we find the following isomorphies

$$\mathbb{Z} \cong_\mathrm{r} \mathbb{Z}\big/_{0\mathbb{Z}} = \mathbb{Z}\big/_{\mathrm{kn}(\zeta)} \cong_\mathrm{r} \mathrm{im}(\zeta) = \mathrm{PRR}(R)$$

where $k \mapsto k + 0\mathbb{Z} = k + \mathrm{kn}(\zeta) \mapsto \zeta(k)$ - which precisely is ζ again. Conversely suppose $\Phi : \mathbb{Z} \cong_\mathrm{r} \mathrm{PRR}(R)$ for some isomorphism Φ. If we had $n \neq 0$, then $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ would be finite. But as we have the isomorphy $\mathbb{Z} \cong_\mathrm{r} \mathrm{PRR}(R) \cong_\mathrm{r} \mathbb{Z}_n$ once more this cannot be (as we thereby find the contradiction $\infty = \#\mathbb{Z} = \#\mathbb{Z}_n = n < \infty$).

(iii) If $n := \mathrm{CHAR}(R) \neq 0$, then we have already proved the minimality of n, that is $n = \min\{\, 1 \leq k \in \mathbb{N} \mid k_R = 0_R \,\}$ in (2.105). Conversely suppoese n is this minimum and denote $c := \mathrm{CHAR}(R)$. As $c_R = 0_R$ and n is minimal with this property we have $n \leq c$. On the other hand we have $\zeta(n) = n_R = 0_R$ and hence $n \in \mathrm{kn}(\zeta) = c\mathbb{Z}$. That is $c \mid n$ and hence $c \leq n$, altogether $n = c = \mathrm{CHAR}(R)$. And $n \neq 0$ is trivial (as n is contained in a subset of $\{k \mid 1 \leq k \in \mathbb{N}\}$). The second equivalence results from the

following isomorphy again (refer to (1.83.(ii))

$$\mathbb{Z}_n \;=\; \mathbb{Z}\big/_{n\mathbb{Z}} \;=\; \mathbb{Z}\big/_{\mathsf{kn}(\zeta)} \;\cong_{\mathsf{r}}\; \mathsf{im}(\zeta) \;=\; \mathsf{PRR}(R)$$

where $k + n\mathbb{Z} = k + \mathsf{kn}(\zeta) \mapsto \zeta(k)$. Thus if $\mathsf{CHAR}R = n \neq 0$ we are done already. Conversely suppose there was some isomorphism Φ such that $\Phi : \mathbb{Z}_n \;\cong_{\mathsf{r}}\; \mathsf{PRR}(\mathbb{Z})$. Then we had (where $c := \mathsf{CHAR}(R)$ again)

$$\mathbb{Z}_c \;=\; \mathbb{Z}\big/_{\mathsf{kn}(\zeta)} \;\cong_{\mathsf{r}}\; \mathsf{im}(\zeta) \;=\; \mathsf{PRR}(R) \;\cong_{\mathsf{r}}\; \mathbb{Z}_n$$

In particular we find $c = \#\mathbb{Z}_c = \#\mathbb{Z}_n = n$ (as $n \neq 0$ and hence $c \neq 0$). That is we have found $n = c = \mathsf{CHAR}(R)$ and $n \neq 0$ has been assumed.

(iv) If $n := \mathsf{CHAR}(R) = 0$, then by (ii) we have $\zeta : \mathbb{Z} \;\cong_{\mathsf{r}}\; \mathsf{PRR}(R)$. And as $\mathsf{PRF}(R)$ is the quotient field of $\mathsf{PRR}(R)$ this implies $\mathbb{Q} \;\cong_{\mathsf{r}}\; \mathsf{PRF}(R)$ under the isomorphy $a/b \mapsto \zeta(a)\zeta(b)^{-1}$. Likewise if $n := \mathsf{CHAR}(R) \neq 0$ then by (iii) we have $\mathbb{Z}_n \;\cong_{\mathsf{r}}\; \mathsf{PRR}(R)$. As R is a field it is a non-zero integral domain. Thus by (i) n is prime. Hence $n\mathbb{Z}$ is a non-zero prime ideal and hence maximal (due to (2.79.(i))), such that $\mathbb{Z}_n$ is a field. As $\mathsf{PRF}(R)$ is the quotient field of (the field) $\mathsf{PRR}(R)$ this implies $\mathbb{Z}_n \;\cong_{\mathsf{r}}\; \mathsf{PRR}(R) = \mathsf{PRF}(R)$. Conversely if $\mathbb{Q} \;\cong_{\mathsf{r}}\; \mathsf{PRF}(R)$, then $\mathsf{CHAR}(R) = 0$ as else $\mathbb{Z}_n \;\cong_{\mathsf{r}}\; \mathsf{PRF}(R) \;\cong_{\mathsf{r}}\; \mathbb{Q}$ (where $n = \mathsf{CHAR}(R) \neq 0$) by what we have just proved. And if $\Phi : \mathbb{Z}_n \;\cong_{\mathsf{r}}\; \mathsf{PRF}(R)$ for some isomorphism Φ, then we have $n_R = n1_R = n\Phi(1 + n\mathbb{Z}) = \Phi(n + n\mathbb{Z}) = \Phi(0 + n\mathbb{Z}) = 0_R$. Thus if $c := \mathsf{CHAR}(R)$, then $n \in \mathsf{kn}(\zeta) = c\mathbb{Z}$ and hence $c \mid n$. On the other hand we have $0_R = c_R = c1_R = c\Phi(1 + n\mathbb{Z}) = \Phi(c + n\mathbb{Z})$. From the injectivity of Φ we get $c + n\mathbb{Z} = 0 + n\mathbb{Z}$ and hence $n \mid c$. As both n and c are positive this only leaves $n = c$.

(v) First suppose we had $c := \mathsf{CHAR}(R) = 0$, then $\zeta : \mathbb{Z} \hookrightarrow R$ would be injective (as $\mathsf{kn}(\zeta) = c\mathbb{Z} = 0$), which contradicts R being finite. Thus we have $c \neq 0$, now let $P := \mathsf{PRR}(R)$, then by (iii) we have $P \;\cong_{\mathsf{r}}\; \mathbb{Z}_c$ and hence $\#P = \#\mathbb{Z}_c = c$. But - being a sub-ring - $P \;\leq_{\mathsf{g}}\; R$ is a subgroup (under the addition $+$ on R). Thus by the theorem of Lagrange (1.7) we have $c = \#P \mid \#R$.

□

Proof of (2.108):

- First of all note that $\mathbb{Z}$ is an euclidean domain (2.71) and hence a PID, which in turn implies that $\mathbb{Z}$ is an UFD (2.79) (iii) and (ii). That is we may use prime decompositions in $\mathbb{Z}$.

- Let $m \in 2 \ldots n$ be the minimal number such that $m \mid n$. That is $qm = n$ for some $1 \leq q < n$. If n is prime, then $n = m$ and conversely if $m < n$ then $n \nmid m$ and $n \nmid q$ such that n is not a prime number. For any $k \in \mathbb{Z}$ the map

$$\mu_k \;:\; \mathbb{Z}_n \;\to\; \mathbb{Z}_n \;:\; a + n\mathbb{Z} \mapsto ka + n\mathbb{Z}$$

is additive (a homomorphism of the additive group $(\mathbb{Z}_n, +)$, as $k(a + b) = ka + kb$ and this equation transfers to $\mathbb{Z}_n$. Let now k be relatively prime to n - that is $1 \in \gcd(k, n)$. Then μ_k even is injective: Suppose $ka + n\mathbb{Z} = kb + n\mathbb{Z}$, then $k(b - a) \in n\mathbb{Z}$ and this means $n \mid k(b - a)$. By (2.64.(iv)) this implies $n \mid (b - a)$ which is $b - a \in n\mathbb{Z}$ and thereby $a + n\mathbb{Z} = b + n\mathbb{Z}$. We are now ready to

prove

$$\mathbb{Z}_n^* \;=\; \{\, k+n\mathbb{Z} \mid 1 \in \gcd(k,n) \,\}$$

If $1 \in \gcd(k,n)$ then $\mu_k : \mathbb{Z}_n \hookrightarrow \mathbb{Z}_n$ is injective. As $\mathbb{Z}_n$ is a finite set, this means μ_k is bijective and hence there is a $j+n\mathbb{Z}$ such that $\mu_k(j+n\mathbb{Z}) = 1+n\mathbb{Z}$. By construction this is $(k+n\mathbb{Z})(j+n\mathbb{Z}) = kj+n\mathbb{Z} = 1+n\mathbb{Z}$ and thereby $k+n\mathbb{Z} = (j+n\mathbb{Z})^{-1}$ is a unit. Conversely suppose $d \mid k$ and $d \mid n$ for some $d \geq 2$. Say $rd = k$ and $sd = n$. Then $s < n$ as $d \geq 2$ and thereby $s+n\,\{\,Z\,\} \neq 0+n\mathbb{Z}$. Yet $sk = s(rd) = r(sd) = rn$ such that $(s+n\mathbb{Z})(k+n\mathbb{Z}) = rn+n\mathbb{Z} = 0+n\mathbb{Z}$. If $k+n\mathbb{Z}$ was a unit we could multiply with its inverse and find $s+n\mathbb{Z} = 0+n\mathbb{Z}$ a contradiction. Thus $k+n\mathbb{Z}$ is a unit if and only if $1 \in \gcd(k,n)$.

- Now the equivalences are easy: If (a) n is a prime number, then any $k \in \mathbb{Z}$ with $1 \leq k < n$ is relatively prime to n. And hence $k+n\mathbb{Z}$ is a unit of $\mathbb{Z}_n$. That is $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{\, 0+n\mathbb{Z} \,\}$ which means $\mathbb{Z}_n$ is a field (b). Any field is an integral domain, so we also get (c). Now if (c) $\mathbb{Z}_n$ is an integral domain, suppose n was not prime, then there were some a, $b \in \mathbb{Z}$ such that $n \mid ab$ but n does neither divide a nor b. Say $qn = ab$, then we have $(a+n\mathbb{Z})(b+n\mathbb{Z}) = qn+n\mathbb{Z} = 0+n\mathbb{Z}$. As n does not divide a we have $a+n\mathbb{Z} \neq 0+n\mathbb{Z}$ and likewise $b+n\mathbb{Z} \neq 0+n\mathbb{Z}$. But this contradicts $\mathbb{Z}_n$ being an integral domain, so we conclude, that n is prime.

□

Proof of (2.109):

(i) Consider a unit $a \in R^*$ of R and suppose $ab = 0$, then $b = a^{-1}0 = 0$ and hence a is no zero-divisor of R. Conversely suppose that $a \notin \mathrm{zD}(R)$ is a non-zero-divisor of R. Then the mapping

$$R \hookrightarrow R \;:\; b \mapsto ab$$

is injective (as $ab = ac$ implies $a(b-c) = 0$ and as $a \notin \mathrm{zD}(R)$ this yields $b-c = 0$ such that $b = c$). But as R is finite any injective map on R also is surjective (and vice versa). Hence there is some $b \in R$ such that $ab = 1$. But this means that $a \in R^*$ is a unit of R.

(ii) For any finite group G we may define the *exponent* of G to be the least common multiple of the orders of its elements

$$\exp(G) \;:=\; \mathrm{lcm}\{\, \mathrm{ord}(x) \mid x \in G \,\}$$

By the Theorem of Lagrange we have $\mathrm{ord}(x) \mid \#G$ for any $x \in G$ such that the least common multiple $\exp(G)$ of the orders is a divisor of $\#G$, as well. By (??) there is some element $g \in G$ such that $\mathrm{ord}(g) = \exp(G)$. Thus if we have $\#G = \exp(G)$ then G is cyclic as it then is generated by the element $g \in G$ with $\mathrm{ord}(g) = \exp(G) = \#G$.

Let now G be a finite subgroup of F^* and let us denote $n := \#G$ and $m := \exp(G)$. Then we need to show $m = n$. As $m \mid n$ we already have $m \leq n$ so it only remains to show $n \leq m$. Now choose any $x \in G \subseteq F^*$, then by construction $x^m = 1$ and hence x is a root of the polynomial $t^m - 1$. Thus we have found n different roots of $t^m - 1$ (namely the elements of G). But the number of roots of $t^m - 1$ is bounded by

$$n \;\leq\; \deg(t^m - 1) \;=\; m$$

(iii) As F has n elements, the multiplicative group $F^* = F \setminus \{0\}$ contains $n-1$ elements. Hence by the theorem of Lagrange (1.9) we get $a^{n-1} = 1$ for any $a \in F^*$. Multiplying this by a we get $a^n = a$. And $0^n = 0$ is clear, as well, such that we get $a^n = a$ for any $a \in F$.

Let $z(t) := t^n - t \in F[t]$, then we have just seen $z(a) = 0$ for any $a \in F$. By (7.54.(iii)) this implies $t - a \mid z$. Now by (2.7.(i)) any $(t-a)F[t]$ is a maximal and hence prime ideal. Therefore the $t - a$ are distinct prime elements of $F[t]$ and therefore

$$p(t) \;:=\; \prod_{a \in F} (t-a) \;\mid\; z$$

by (2.59.(vi)). But as F contains n elements, $p(t) \in F[t]$ is of degree n, just like $z(t)$. Suppose $z(t) = p(t) \cdot q(t)$, then $\deg(q) = \deg(z) - \deg(q) = 0$ such that $q(t) = u$ for some $q \in F$. But both p and z are monic, so q must have leading coefficient $u = 1$, as well. And this is $q(t) = 1$ such that we find the identity $z(t) = p(t)$ of these two polynomials.

(iv) If $f = pa$ then we easily have $(f + p^n S)(p^{n-1} + p^n S) = p^n a + p^n S = 0 + p^n S$. And as S is an integral domain we have $p^n \not\mid p^{n-1}$ or in other words $p^{n-1} + p^n S \neq 0 + p^n S$. And hence $f + p^n S$ is a zero-divisor of $S/p^n S$. Conversely suppose $(f + p^n S)(g + p^n S) = 0 + p^n S$ for some $g + p^n S \neq 0 + p^n S$. This means $p^n \not\mid g$ and hence we obtain a well-defined $l \in 1 \ldots n-1$ by letting

$$l \;:=\; g[p] \;:=\; \max\Big\{ k \in \mathbb{N} \mid p^k \mid g \Big\}$$

If we now write $g = p^l b$ then by assumption we have $p^n \mid fg = fp^l b$ and hence $p \mid p^{n-l} \mid fb$. As p is prime we get $p \mid f$ or $p \mid b$. But as l has been chosen maximally $p \mid b$ is absurd, which only leaves $p \mid f$.

(v) As $R \neq 0$ (because of $p^n S \subseteq pS \neq S$) we have already seen the inclusions $\mathrm{nil}(R) \subseteq \mathrm{zd}(R) \subseteq R \setminus R^*$ in (1.47.(ii)). And by (ii) we already know $\mathrm{zd}(R) = (p + p^n S)R$. And if $pa + p^n S \in \mathrm{zd}(R)$ then

$$(pa + p^n S)^n \;=\; p^n a^n + p^n S \;=\; 0 + p^n S$$

which also proves $\mathrm{zd}(R) \subseteq \mathrm{nil}(R)$. Thus it only remains to prove the inclusion $R \setminus R^* \subseteq (p + p^n S)R$. Thus consider $x = f + p^n S \notin R^*$, in particular we have $f \notin S^*$ (as else $x^{-1} = f^{-1} + p^n S$). Thus f has a true (i.e. $r \geq 1$) prime factorization

$$f \;=\; \alpha q \quad \text{where} \quad q \;:=\; \prod_{i=1}^{r} q_i$$

with $\alpha \in S^*$ and $q_i \in S$ prime. Now suppose that p is not associated to any of the q_i (formally that is $\neg(p \approx q_i)$ for any $i \in 1 \ldots r$) then we had $\gcd(p^n, q) = 1$. The lemma of Bezout (2.83.(iii)) then implies

$$p^n S + qS \;=\; \gcd(p^n, q)S \;=\; S$$

Therefore there are a and $b \in S$ such that $ap^n + bq = 1$ or in other words $bq = 1 - ap^n$. Now let $g := ap^n + \alpha^{-1} b$, then it is clear that

$$fg \;=\; \alpha q(ap^n + \alpha^{-1} b) \;=\; (\alpha a q - a)p^n + 1$$

And hence $(f+p^nS)(g+p^nS) = 1+p^nS$ which implies $x^{-1} = g+p^nS$ and in particular $x \in R^*$, a contradiction. Hence there has to be some $i \in 1\ldots r$ such that $p \approx q_i$. And therefore we find $p \approx q_i \mid f$ such that $p \mid f$, or in other words again $f \in (p+p^nS)R$. Thus we got

$$\text{NIL}(R) \;=\; \text{ZD}(R) \;=\; R \setminus R^* \;=\; (p+p^nS)\,R$$

Now consider any prime ideal $\mathfrak{p} \trianglelefteq_{\text{i}} R$, then it is clear that $\text{NIL}(R) \subseteq \mathfrak{p} \subseteq R \setminus R^*$. But by the equality $\text{NIL}(R) = R \setminus R^*$ this means $\mathfrak{p} = \text{NIL}(R)$. Therefore $\text{NIL}(R)$ is the one and only prime ideal of R. But $\text{NIL}(R)$ already is maximal - if $\text{NIL}(R) \subset \mathfrak{a} \trianglelefteq_{\text{i}} R$, then there is some $a \in \mathfrak{a} \cap R^*$ and hence $\mathfrak{a} = R$. Thus we have also proved the second equality

$$\text{Spec}(R) \;=\; \text{Smax}(R) \;=\; \{\,\text{NIL}(R)\,\}$$

(vi) We will prove the claim in several steps: (1) given any commutative ring R and any ideal $\mathfrak{a} \trianglelefteq_{\text{i}} R$ let us first denote the following set

$$X_n(R,\mathfrak{a}) \;:=\; \{\,\mathfrak{p} \in \text{Spec}(R) \mid \mathfrak{a} \subseteq \mathfrak{p},\ \#R/\mathfrak{p} \leq n\,\}$$

Then it is clear that $\mathfrak{a} \subseteq \mathfrak{b} \implies X_n(R,\mathfrak{b}) \subseteq X_n(R,\mathfrak{a})$ (because if we are given $\mathfrak{p} \in X_n(R,\mathfrak{b})$, then $\mathfrak{a} \subseteq \mathfrak{b} \subseteq \mathfrak{p}$ and hence $\mathfrak{a} \subseteq \mathfrak{p}$, such that $\mathfrak{p} \in X_n(R,\mathfrak{a})$). Further $X_n(R,\mathfrak{a}\,\mathfrak{b}) \subseteq X_n(R,\mathfrak{a}) \cup X_n(R,\mathfrak{b})$ (because if we are given $\mathfrak{p} \in X_n(R,\mathfrak{a}\,\mathfrak{b})$ then $\mathfrak{a}\,\mathfrak{b} \subseteq \mathfrak{p}$ and as $\mathfrak{p}$ is prime this implies $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$ such that $\mathfrak{p} \in X_n(R,\mathfrak{a})$ or $\mathfrak{p} \in X_n(R,\mathfrak{b})$). Now suppose $\mathfrak{a} \subseteq \mathfrak{b} \trianglelefteq_{\text{i}} R$, then we will prove

$$\#X_n(R,\mathfrak{b}) \;=\; \#X_n\left(R\Big/_{\mathfrak{a}}, \mathfrak{b}\Big/_{\mathfrak{a}}\right)$$

This is clear once we prove that $\mathfrak{p} \mapsto \mathfrak{p}/\mathfrak{a}$ is a bijection from $X_n(R,\mathfrak{b})$ to $X_n(R/\mathfrak{a},\mathfrak{b}/\mathfrak{a})$. But by the correspondence theorem (1.66) (and the remarks following it) $\overline{\mathfrak{p}} \trianglelefteq_{\text{i}} R/\mathfrak{a}$ is prime if and only if $\overline{\mathfrak{p}} = \mathfrak{p}/\mathfrak{a}$ for some $\mathfrak{p} \trianglelefteq_{\text{i}} R$ prime, with $\mathfrak{a} \subseteq \mathfrak{p}$. And due to the correspondence theorem we also have $\mathfrak{b} \subseteq \mathfrak{p}$ if and only if $\mathfrak{b}/\mathfrak{a} \subseteq \mathfrak{p}/\mathfrak{a}$. Finally we've got the third isomorphism theorem (1.83.(iv)) which provides the isomorphy $R/\mathfrak{p} \;\cong_{\text{r}}\; (R/\mathfrak{a})/(\mathfrak{p}/\mathfrak{a})$. In particular we have $\#R/\mathfrak{p} = \#(R/\mathfrak{a})/(\mathfrak{p}/\mathfrak{a})$. Thus $\mathfrak{p} \mapsto \mathfrak{p}/\mathfrak{a}$ is well-defined and surjective. But the injectivity is clear (by the correspondence theorem) and hence it is bijective. In a second step (2) let us now denote the set

$$\mathcal{A} \;:=\; \{\,\mathfrak{a} \trianglelefteq_{\text{i}} R \mid \#X_n(R,\mathfrak{a}) = \infty\,\}$$

Suppose $\mathcal{A} \neq \emptyset$ was non-empty, then (as R is noetherian) there would be a maximal element $\mathfrak{a}^* \in \mathcal{A}^*$. We now claim that this maximal element $\mathfrak{a}^*$ is prime. It is clear, that $\mathfrak{a}^* \neq R$, as $R/R = 0$ has not a single prime ideal, in particular $\#X_n(R,R) = 0$. Thus suppose there would be some $a, b \in R$ such that $ab \in \mathfrak{a}^*$ but $a, b \notin \mathfrak{a}^*$. Then we let $\mathfrak{a} := \mathfrak{a}^* + aR$ and $\mathfrak{b} := \mathfrak{a}^* + bR$ and thereby get $\mathfrak{a}^* \subset \mathfrak{a}, \mathfrak{b}$ and $\mathfrak{a}\,\mathfrak{b} \subseteq \mathfrak{a}^*$. Thus by the inclusions in (1) we would find

$$X_n(R,\mathfrak{a}^*) \;\subseteq\; X_n(R,\mathfrak{a}\,\mathfrak{b}) \;\subseteq\; X_n(R,\mathfrak{a}) \cup X_n(R,\mathfrak{b})$$

But as $\mathfrak{a}^*$ is maximal in $\mathcal{A}$ we have $\mathfrak{a}, \mathfrak{b} \notin \mathcal{A}$. That is both $X_n(R,\mathfrak{a})$ and $X_n(R,\mathfrak{b})$ are finite. Thus by the above inclusion $X_n(R,\mathfrak{a}^*)$ is finite, too, in contradiction to $\mathfrak{a}^* \in \mathcal{A}$ - thus $\mathfrak{a}^*$ is prime. For

the third step (3) let $Q := R/\mathfrak{a}^*$, then by (2) Q is an integral domain. And if $0 \neq \mathfrak{u} \trianglelefteq_{\mathrm{i}} Q$ is a non-zero ideal, then by the correspondence therorem there is some ideal $\mathfrak{b} \trianglelefteq_{\mathrm{i}} R$ with $\mathfrak{a}^* \subset \mathfrak{b}$ such that $\mathfrak{u} = \mathfrak{b}/\mathfrak{a}^*$. But as $\mathfrak{a}^*$ has been maximal the equality in (1) yields

$$\#X_n(Q,\mathfrak{u}) \;=\; X_n\left(R\Big/_{\mathfrak{a}^*}, \mathfrak{b}\Big/_{\mathfrak{a}^*}\right) \;=\; \#X_n(R,\mathfrak{b}) \;<\; \infty$$

(4) the same reasoning yields $\#X_n(Q,0) = \#X_n(R,\mathfrak{a}^*) = \infty$, such that Q is infinite (if it was finite, that so was its spectrum and hence the subset $X_n(Q,0)$ was finite as well). Thus we may choose pairwise distinct elements $f_1,\ldots,f_{n+1} \in Q$ and let

$$f \;:=\; \prod_{i\neq j}(f_i - f_j) \;\in\; Q$$

as $f_i - f_j \neq 0$ for any $i \neq j$ and Q is an integral domain we have $f \neq 0$ as well. Now consider any prime ideal $\mathfrak{q} \trianglelefteq_{\mathrm{i}} Q$, if we have $f \notin \mathfrak{q}$ then (as $\mathfrak{q}$ is an ideal) for any $i \neq j \in 1\ldots n+1$ we have $f_i - f_j \notin \mathfrak{q}$. Thus for any $i \neq j \in 1\ldots n+1$ we have $f_i + \mathfrak{q} \neq f_j + \mathfrak{q}$. That is $Q/\mathfrak{q}$ contains (at least) $n+1$ distinct elements and hence $\mathfrak{q} \notin X_n(Q,0)$. Thus for any $\mathfrak{q} \in X_n(Q,0)$ we necessarily have $f \in \mathfrak{q}$ and hence

$$X_n(Q,0) \;=\; X_n(Q,fQ)$$

But as $f \neq 0$ we have $fQ \neq 0$ such that (3) yields $\#X_n(Q,fQ) < \infty$. By the equalities above this means $\infty = \#X_n(R,\mathfrak{a}^*) = \#X_n(Q,0) = X_n(Q,fQ) < \infty$ a contradiction. This means that our assumption $\mathcal{A} \neq \emptyset$ has to be false. In other words $\mathcal{A} = \emptyset$ and in particular $0 \notin \mathcal{A}$. That is $\#X_n(R,0) < \infty$ which is a trivial reformulation of the claim.

□

Proof of (2.112):
The implications (a) $\Longrightarrow$ (b) and (a) $\Longrightarrow$ (c) are trivial. Thus it only remains to check the converse implications. The proof of (c) $\Longrightarrow$ (a) is elementary and has been given in (2.109.(i)). Yet (b) $\Longrightarrow$ (a) requires knowledge of group actions (which will be presented in book 2, or any other standard text on algebra) and cyclotomic fields (which also will be presented in book 2, or any standard text on Galois theory). Never the less we want to give a proof of (b) $\Longrightarrow$ (a) and the reader is asked to refer to the sources given for the statements not contained in this text:

Let us regard the multiplicative group $F^* = F \setminus \{0\}$ (this truly is a group, as F is a skew-field) of F. And let us denote the *center* of the ring F by

$$C \;:=\; \{\, a \in F \mid \forall\, x \in F : ax = xa \,\}$$

It is obvious that $C \leq_{\mathrm{r}} F$ is a commutative sub-ring of F and hence it even is a field. Thus $(F,+)$ is a C-vectorspace under its own multiplication. And as F is finite it clearly has to be finite-dimensional $n := \dim_C F < \infty$. If we denote $q := \#C$ then this implies

$$\#F^* \;=\; \#F - 1 \;=\; \#C^n - 1 \;=\; q^n - 1$$

For any $x \in E^*$ let us now denote the *conjugacy class*, the *centralizer* and the centralizer appended by

0, using the notations

$$\begin{aligned} \mathrm{con}(x) &:= \left\{ yxy^{-1} \mid y \in E^* \right\} \\ \mathrm{CEN}(x) &:= \{ y \in E^* \mid xy = yx \} \\ C(x) &:= \{ y \in E \mid xy = yx \} \end{aligned}$$

It is well-known from group theory that the conjugacy classes $\mathrm{con}(x)$ form a partition of F^* and that $\mathrm{con}(a) = \{ a \}$ for any $a \in C$. Thus let us denote by $X \subseteq F \setminus C$ a representing system of the conjugacy classes, that is $X \longleftrightarrow \{ \mathrm{con}(x) \mid x \in F \setminus C \}$ under $x \mapsto \mathrm{con}(x)$. As the conjugacy classes form a partition of F^* we find the equality

$$\begin{aligned} q^n - 1 \;=\; \#F^* &= \sum_{0 \neq a \in C} \#\mathrm{con}(a) + \sum_{x \in X} \#\mathrm{con}(x) \\ &= \#C^* + \sum_{x \in X} \#\mathrm{con}(x) \\ &= (q-1) + \sum_{x \in X} \#\mathrm{con}(x) \end{aligned}$$

It is clear that $(C(x), +)$ is a subgroup of the additive group $(F, +)$. But it even is a C-subspace of F, we denote its (finite) dimension by $n(x) := \dim_C C(x)$, then we get

$$\#\mathrm{CEN}(x) \;=\; \#C(x) - 1 \;=\; \#C^{n(x)} - 1 \;=\; q^{n(x)} - 1$$

We now apply the orbit formula $\#F^* = \#\mathrm{con}(x) \cdot \#\mathrm{CEN}(x)$. Yet as $\#\mathrm{con}(x)$ is an iteger we find the divisibility $\#\mathrm{CEN}(x) \mid \#F^*$. Using division with remainder we obtain

$$q^n - 1 : q^{n(x)} - 1 \;=\; q^{n-n(x)} + q^{n-2n(x)} + \cdots + q^{n-r(x)n(x)}$$

As this division leaves no remainder we necessarily find $n = r(x)n(x)$, i.e. $n(x)$ divides n. On the other hand the orbit formula yields

$$\#\mathrm{con}(x) \;=\; \frac{q^n - 1}{q^{n(x)} - 1}$$

Substituting this into our partition formula for the cardinality of F^* we find

$$q^n - 1 \;=\; (q-1) + \sum_{x \in X} \frac{q^n - 1}{q^{n(x)} - 1}$$

This is the point where the cyclotomic polynomials $\Phi_m \in \mathbb{Z}[t]$ come into play. Let $m \in \mathbb{N}$ and $\omega_m := \exp(2\pi i/m) \in \mathbb{C}$, further denote $k \perp m \;:\Longleftrightarrow\; k \in 1 \ldots m$ and $\gcd(k, m) = \pm 1$. Then the m-th *cyclotomic polynomial* is defined to be

$$\Phi_m \;:=\; \prod_{k \perp m} (t - \omega_m^k)$$

In book 2 it will be shown that $\Phi_m \in \mathbb{Z}[t]$ has integer coefficients in fact and (if we denote $d \mid m \;:\Longleftrightarrow\; d \in 1 \ldots m$ and $d \mid m$) satisfies

$$\prod_{d \mid m} \Phi_d \;=\; t^m - 1$$

We now assume $F \neq C$ (i.e. F is not commutative) and regard any $x \in X$. It is clear that we find $\Phi_n(q) \mid q^n - 1$. But as $x \notin C$ we get $\#\mathrm{con}(x) \neq 1$ and hence $n \neq n(x)$ on the other hand we have seen $n(x) \mid n$ and hence

$$(t^{n(x)} - 1)\Phi_n \;=\; \left(\prod_{d \mid n(x)} \Phi_d\right)\Phi_n \;\Big|\; \prod_{d \mid n} \Phi_d \;=\; t^n - 1$$

Thus we get $\Phi_n(q) \mid (q^n - 1)/(q^{n(x)} - 1)$, too and substituting this and $\Phi_n(q) \mid q^n - 1$ into the equation of the partition we obtain

$$\Phi_n(q) \;\Big|\; (q^n - 1) - \sum_{x \in X} \frac{q^n - 1}{q^{n(x)} - 1} \;=\; q - 1$$

In particular we get $\Phi_n(q) \leq q - 1$. But this clearly cannot be - as $q \geq 2$ (at least 0 and $1 \in C$) we see by the triange inequality that $|q - 1| < |q - w_n^k|$ for any $k \in 1 \ldots n - 1$. Hence we arrived at a contradiction (to $C \neq F$)

$$q - 1 \;\geq\; |\Phi_n(q)| \;=\; \prod_{k \perp n} |q - \omega_n^k| \;>\; \prod_{k \perp n} |q - 1| \;\geq\; q - 1$$

□

Proof of (2.114):

(i) R^* and $\mathrm{NZD}(R)$ are multiplicatively closed, due to (1.47). And if conversely $uv \in R^*$, then there is some $a \in R$ such that $1 = a(uv) = u(av)$. Hence we also have $u \in R^*$. Likewise, if $uv \in \mathrm{NZD}(R)$ and $a \in R$ then $au = 0$ implies $auv = 0$ and hence $a = 0$ such that $u \in \mathrm{NZD}(R)$.

(iii) $1 = 1 \cdot 1 \in UV$ is clear and if u, $u' \in U$ and v, $v' \in V$, then for any uv and $u'v' \in UV$ we get $(uv)(u'v') = (uu')(vv') \in UV$ again.

(iv) Immediate: if a and $b \in \mathfrak{a}$ then $(1 + a)(1 + b) = 1 + (a + b + ab) \in 1 + \mathfrak{a}$.

(v) Clearly $1 \in \varphi(U)$, as $1 \in U$ and $\varphi(1) = 1$. And if p, $q \in \varphi(U)$ then there are u, $v \in U$ such that $p = \varphi(u)$ and $q = \varphi(v)$. Hence $pq = \varphi(u)\varphi(v) = \varphi(uv) \in \varphi(U)$ since $uv \in U$. Likewise $1 \in \varphi^{-1}(V)$ is clear, as $\varphi(1) = 1 \in V$. And if u, $v \in \varphi^{-1}(V)$ then $\varphi(u)$, $\varphi(v) \in V$. thereby we get $uv \in \varphi^{-1}(V)$ from $\varphi(uv) = \varphi(u)\varphi(v) \in V$. So let us finally suppose V is saturated and $uv \in \varphi^{-1}(V)$. Then $\varphi(uv) = \varphi(u)\varphi(v) \in V$ implies $\varphi(u) \in V$ and hence $u \in \varphi^{-1}(V)$, as well.

(vi) As $\mathcal{U} \neq \emptyset$ there is some $1 \in U \in \mathcal{U}$ and hence $1 \in \bigcup \mathcal{U}$. And if now $uv \in \bigcup \mathcal{U}$ then there are some U, $V \in \mathcal{U}$ such that $u \in U$ and $v \in V$. As $\mathcal{U}$ is a chain we may assume $U \subseteq V$ and hence $u \in V$. This yields $uv \in V$ and hence $uv \in \bigcup \mathcal{U}$.

(vii) Since $1 \in U$ for any $U \in \mathcal{U}$ we also have $1 \in \bigcap \mathcal{U}$. And if u, $v \in \bigcap \mathcal{U}$, then u, $v \in U$ for any $U \in \mathcal{U}$. Thereby $uv \in U$, as U is multiplicatively closed and hence $uv \in \bigcap \mathcal{U}$. Likewise if any $U \in \mathcal{U}$ is saturated, then $uv \in \bigcap \mathcal{U}$ implies $uv \in U$ and hence $u \in U$ for any $U \in \mathcal{U}$. And the latter translates into $u \in \bigcap \mathcal{U}$ again.

(viii) Clearly $1 = u^0 \in U$ and if u^i and $u^j \in U$ then also $u^i u^j = u^{i+j} \in U$. That is U is a multiplicatively closed set with $u \in U$. And if conversely $V \subseteq R$ is any multiplicatively closed set with $u \in V$,

then by induction on k we also find $u^k \in V$ and hence $U \subseteq V$. Together this proves, that U is the smallest multiplicatively closed set containing u.

(ix) Let us define $\overline{U}$ to be the set given, then we need to show that $\overline{U}$ is the intersection of all saturated multiplicatively closed subsets $V \subseteq R$ containing U. "$\subseteq$": Thus consider any saturated multiplicatively closed $V \subseteq R$ with $U \subseteq V$. If now $a \in \overline{U}$ then there are $b \in R$ and $u, v \in U$ such that $uab = uv \in U \subseteq V$. In particular $a(ub) = uab \in V$ and as V is saturated this implies $a \in V$. Hence $\overline{U} \subseteq V$ is contained in any such V. "$\supseteq$": If $a \in U$ that $1a1 = 1a$ and hence $a \in \overline{U}$. Hence we have $U \subseteq \overline{U}$ so it remains to prove that $\overline{U}$ is saturated multiplicatively closed. Thus consider a and $a' \in \overline{U}$, that is $uab = uv$ and $u'a'b' = u'v'$ for sufficient b, $b' \in R$ and u, v, u', $v' \in U$. Then $(uu')aa'(bb') = (uu')(vv')$ and hence $aa' \in \overline{U}$, as uu', $vv' \in U$. Conversely suppose $aa' \in \overline{U}$, that is $u(aa')b = uv$ for sufficient $b \in R$, u, $v \in U$. Then $ua(a'b) = u(aa')b = uv$ and hence $a \in \overline{U}$.

□

Proof of (2.115):
We first prove (b) $\implies$ (a): consider any prime ideal $\mathfrak{p} \trianglelefteq_{\mathfrak{i}} R$, then $1 \in R \setminus \mathfrak{p}$, as $1 \in \mathfrak{p}$ would imply $\mathfrak{p} = R$ which is disallowed. And as $\mathfrak{p}$ is both, *prime* and an *ideal* we get the following equivalence for all u, $v \in R$

$$uv \in \mathfrak{p} \iff u \in \mathfrak{p} \text{ or } v \in \mathfrak{p}$$

Hence if we go to complements (i.e. if we negate this equivelency) then we find that $R \setminus \mathfrak{p}$ is a saturated multiplicative set, since

$$uv \in R \setminus \mathfrak{p} \iff u \in R \setminus \mathfrak{p} \text{ or } v \in R \setminus \mathfrak{p}$$

And from this we find that $R \setminus \bigcup \mathcal{P}$ is a saturated multiplicative set, as it is the intersection of such sets $R \setminus \mathfrak{p}$ for $\mathfrak{p} \in \mathcal{P}$, formally

$$R \setminus \bigcup \mathcal{P} = R \setminus \bigcup_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p} = \bigcap_{\mathfrak{p} \in \mathcal{P}} R \setminus \mathfrak{p}$$

Next we prove (a) $\implies$ (a): fix $a \in R \setminus U$ then also $aR \subseteq R \setminus U$: consider $b \in R$, then $ab \in U$ - because of the saturation of U - would imply $a \in U$, in contradiction to $a \notin U$. And as U is multiplicatively closed we max choose an ideal $\mathfrak{p}(a)$ maximal among the ideals $\mathfrak{b}$ with $aR \subseteq \mathfrak{b} \subseteq R \setminus U$. And this $\mathfrak{p}(a)$ is prime (for all this refer to (2.18.(iv))). Thus we get

$$R \setminus U \subseteq \bigcup_{a \notin U} aR \subseteq \bigcup_{a \notin U} \mathfrak{p}(a) \subseteq R \setminus U$$

$$\implies U = R \setminus \bigcup \{ \mathfrak{p}(a) \mid a \notin U \}$$

□

Proof of (2.116):

- We will first prove that $\sim$ is an equivalence relation: the reflexivity is due to $1 \in U$, as $u1a = u1a$ implies $(u, a) \sim (u, a)$. For the symmetry suppose $(u, a) \sim (v, b)$, i.e. there is some $w \in U$ such that $vwa = uwb$. As $=$ is symmetric we get $uwb = vwa$ and this is $(v, b) \sim (u, a)$ again. To finally prove the transitivity we regard $(u, a) \sim (v, b)$ and $(v, b) \sim (w, c)$. That is there are p, $q \in U$ such that $pva = pub$ and $qwb = qvc$. Since p, q and $v \in U$ we also have $pqv \in U$. Now

compute $(pqv)wa = qw(pva) = qw(pub) = pu(qwb) = pu(qvc) = (pqv)uc$, this yields that truly $(u,a) \sim (w,c)$ are equivalent, too.

- Next we need to check that the operations $+$ and $\cdot$ are well-defined. Suppose $a/u = a'/u'$ and $b/v = b'/v'$ that is there are p and $q \in U$ such that $pu'a = pua'$ and $qv'b = qvb'$. Then we let $w := pq \in U$ and compute

$$\begin{aligned} u'v'w(av+bu) &= vv'q(pu'a) + uu'p(qv'b) \\ &= vv'q(pua') + uu'p(qvb') \\ &= uvw(a'v' + u'b') \\ u'v'wab &= (pu'a)(qv'b) \\ &= (pua')(qvb') \\ &= uvwa'b' \end{aligned}$$

 That is $(a/u)+(b/v) = (av+bu)/uv = (a'v'+b'u')/u'v' = (a'/u')+(b'/v')$ and $(a/u)(b/v) = ab/uv = a'b'/u'v' = (a'/u')(b'/v')$ respectively. And this is just the well-definedness of sum and product.

- Next it would be due to verify that $U^{-1}R$ thereby becomes a commutative ring. That is we have to check that $+$ and $\cdot$ are associative, commutative and satisfy the distributivity law. Further that for any $a/u \in U^{-1}R$ we have $a/u + 0/1 = a/u$ and $a/u + (-a)/u = 0/1$ and finally that $a/u \cdot 1/1 = a/u$. But this can all be done in straightforward computations, that we wish to omit here.

- It is obvious that thereby κ becomes a homomorphism of rings, $\kappa(0) = 0/1$ is the zero-element and $\kappa(1) = 1/1$ is the unit element. Further $\kappa(a+b) = (a+b)/1 = (a1+b1)/1\cdot 1 = a/1 + b/1 = \kappa(a) + \kappa(b)$ and $\kappa(ab) = ab/1 = ab/1\cdot 1 = (a/1)(b/1) = \kappa(a)\kappa(b)$.

- Next we wish to prove that κ is injective, if and only if $U \subseteq \text{NZD}(R)$. To do this we take a look at the kernel of κ

$$\begin{aligned} \ker(\kappa) &= \{\, a \in R \mid a/1 = 0/1 \,\} \\ &= \{\, a \in R \mid \exists\, u \in U : au = 0 \,\} \end{aligned}$$

 By (1.80.(i)) κ is injective iff $\ker(\kappa) = \{0\}$. That is iff for any $u \in U$ we get $au = 0 \implies a = 0$. And this is just a reformulation of $U \subseteq \text{NZD}(R)$.

- So it remains to prove that κ is bijective if and only if $U \subseteq R^*$. First suppose $U \subseteq R^* \subseteq \text{NZD}(R)$ by (1.47). Then as we have just seen κ is injective. Now consider any $a/u \in U^{-1}R$, then

$$\frac{a}{u} = \frac{au^{-1}u}{u} = \frac{au^{-1}}{1} = \kappa(au^{-1}) \in \operatorname{im}(\kappa)$$

 Hence we found that κ also is surjective. Conversely suppose that κ is bijective. In particular κ is injective and hence $U \subseteq \text{NZD}(R)$. But κ also is surjective, that is for any $u \in U$ there is some $b \in R$ such that $1/u = \kappa(b) = b/1$. That is there is some $w \in U$ such that $w = uwb$. Equivalently

$w(ub-1)=0$, but as $w \in \text{NZD}(R)$ this implies $ub=1$ and hence $u \in R^*$. As u has been arbitrary we found $U \subseteq R^*$.

□

Proof of (3.121):

- We will first prove that $\sim$ is an equivalence relation: the reflexivity is due to $1 \in U$, as $u1x = u1x$ implies $(u,x) \sim (u,x)$. For the symmetry suppose $(u,x) \sim (v,y)$, i.e. there is some $w \in U$ such that $vwx = uwy$. As $=$ is symmetric we get $uwy = vwx$ and this is $(v,y) \sim (u,x)$ again. To finally prove the transitivity we regard $(u,x) \sim (v,y)$ and $(v,y) \sim (w,z)$. That is there are p, $q \in U$ such that $pvx = puy$ and $qwy = qvz$. Since p, q and $v \in U$ we also have $pqv \in U$. Now compute $(pqv)wx = qw(pvx) = qw(puy) = pu(qwy) = pu(qvz) = (pqv)uz$, this yields that truly $(u,x) \sim (w,z)$ are equivalent, too.

- Next we need to check that the addition is well-defined. Suppose $x/u = x'/u'$ and $y/v = y'/v'$ that is there are p and $q \in U$ such that $pu'x = pux'$ and $qv'y = qvy'$. Then we let $w := pq \in U$ and compute

$$\begin{aligned} u'v'w(vx+uy) &= vv'q(pu'x) + uu'p(qv'y) \\ &= vv'q(pux') + uu'p(qvy') \\ &= uvw(v'x' + u'y') \end{aligned}$$

 That is $(x/u)+(y/v) = (vx+uy)/uv = (v'x'+u'y')/u'v' = (x'/u')+(y'/v')$ which is the well-definedness of the addition. For the R-scalar multiplication we need to show that $a(x/u) = ax/u = ax'/u' = a(x'/u')$. But by taking $w = p$ this is easy to see

$$pu'(ax) \;=\; a(pu'x) \;=\; a(pux') \;=\; pu(ax')$$

 which is the equivalence $(u,ax) \sim (u',ax')$. Likewise for the $U^{-1}R$-scalar multiplication we need to show that $(a/u)(y/v) = ay/uv = ay'/uv' = (a/u)(y'/v')$. But taking $w = q$ this time, we prove the equivalence $(uv,ay) \sim (uv',ay')$ by computing

$$q(uv')(ay) \;=\; au(qv'y) \;=\; au(qvy') \;=\; q(uv)(ay')$$

- Next we have to prove that $U^{-1}M$ truly becomes an $U^{-1}R$-module. We start by proving the properties of a commutative group: associativity, commutativity and the existence of the neutral element $0/1$ and the inverse element $-x/u$ of x/u

$$\begin{aligned} \left(\frac{x}{u}+\frac{y}{v}\right)+\frac{z}{w} &= \frac{vx+uy}{uv}+\frac{z}{w} \\ &= \frac{vwx+uwy+uvz}{uvw} \\ &= \frac{x}{u}+\frac{wy+vz}{vw} \\ &= \frac{x}{u}+\left(\frac{y}{v}+\frac{z}{w}\right) \\ \frac{x}{u}+\frac{y}{v} &= \frac{vx+uy}{uv} = \frac{uy+vx}{vu} \end{aligned}$$

$$\begin{aligned} &= \frac{y}{v}+\frac{x}{u} \\ \frac{x}{u}+\frac{0}{1} &= \frac{1x+u0}{u\cdot 1} = \frac{x}{u} \\ \frac{x}{u}+\frac{-x}{u} &= \frac{ux+u(-x)}{u\cdot u} = \frac{x+(-x)}{u} \\ &= \frac{0}{u} = \frac{0}{1} \end{aligned}$$

Next we have to check the compatibility conditions of the scalar multiplication with the addition on $U^{-1}M$. Again this can be done in straightforward computations

$$\begin{aligned} \frac{a}{u}\left(\frac{y}{v}+\frac{z}{w}\right) &= \frac{a}{u}\frac{wy+vz}{vw} = \frac{a(wy+vz)}{uvw} \\ &= \frac{uway+uvaz}{uvuw} = \frac{ay}{uv}+\frac{az}{uw} \\ &= \frac{a}{u}\frac{y}{v}+\frac{a}{u}\frac{z}{w} \\ \left(\frac{a}{u}+\frac{b}{v}\right)\frac{z}{w} &= \frac{va+ub}{uv}\frac{z}{w} = \frac{vaz+ubz}{uvw} \\ &= \frac{vaz}{vuw}+\frac{ubz}{uvw} = \frac{az}{uw}+\frac{bz}{vw} \\ &= \frac{a}{u}\frac{z}{w}+\frac{b}{v}\frac{z}{w} \\ \left(\frac{a}{u}\frac{b}{v}\right)\frac{z}{w} &= \left(\frac{ab}{uv}\right)\frac{z}{w} = \frac{abz}{uvw} \\ &= \frac{a}{u}\frac{bz}{vw} = \frac{a}{u}\left(\frac{b}{v}\frac{z}{w}\right) \\ \frac{1}{1}\frac{x}{u} &= \frac{1x}{1u} = \frac{x}{u} \end{aligned}$$

- As $\kappa : R \to U^{-1}R : a \mapsto a/1$ is a homomorphism of rings and $U^{-1}M$ is an $U^{-1}R$-module it also becomes an R-module under the following scalar multiplication

$$a\frac{x}{u} = \kappa(a)\frac{x}{u} = \frac{a}{1}\frac{x}{u} = \frac{ax}{u}$$

- Next we would like to show that $\kappa : M \to U^{-1}M : x \mapsto x/1$ is an R-module homomorphism. But this is obvious for any x, $y \in M$ and any $a \in R$ we get: $\kappa(ax) = ax/1 = a(x/1) = a\kappa(x)$ and $\kappa(x+y) = (x+y)/1 = (1x+1y)/(1\cdot 1) = x/1 + y/1 = \kappa(x)+\kappa(y)$.

- Let us now prove that κ is injective if and only if $U \subseteq \text{NZD}(M)$: note that κ is injective, iff $\ker(\kappa) = 0$ that is if $x/1 = 0/1$ implies that $x = 0$. But by definition $x/1 = 0/1$ means $wx = w0 = 0$ for some $w \in U$. That is κ is injective if and only if U and the set $R \setminus \text{NZD}(M) = \{\, a \in R \mid \exists\, x \in M \text{ such that } x \neq 0 \text{ and } ax = 0 \,\}$ are disjoint. In other words that is $U \subseteq \text{NZD}(M)$.

- Let us finally assume that $U \subseteq R^*$. Then (as $M \neq 0$) it is clear that $U \subseteq \text{NZD}(M)$ such that κ already is injective. It remains to prove the surjectivity. Hence consider any $y/u \in U^{-1}M$. Then we chose $w = 1$ and $x = u^{-1}y$ from which we find $wux = uu^{-1}y = y = wy$ such that $\kappa(x) = x/1 = y/u$. Together we derived the bijectivity of κ.

□

Proof of (3.122):
By definition we have $x/u = 0/1$ iff there is some $w \in U$ such that $1wx = uw0 = 0$. That is if and only if $wx = 0$. Next - due to the commutativity of R - we have $u(vx) = (uv)x = (vu)x$, so choosing $w = 1$ we see that $vx/vu = x/u$. And the third equality calls for induction: for $n = 1$ there is nothing to prove, for $n = 2$ this is precisely the definiton of the addition in $U^{-1}M$: $x_1/u_1 + x_2/u_2 = (u_2x_1 + u_1x_2)/(u_1u_2)$. So for the induction step use the notation of $u = u_1 \dots u_n$ and $\widehat{u}_i = u/u_i$ as introduced in the remark

$$\begin{aligned}\frac{x_1}{u_1} + \dots + \frac{x_n}{u_n} + \frac{x_{n+1}}{u_{n+1}} &= \frac{\widehat{u}_1x_1 + \dots + \widehat{u}_nx_n}{u} + \frac{x_{n+1}}{u_{n+1}} \\ &= \frac{\widehat{u}_1u_{n+1}x_1 + \dots + \widehat{u}_nu_{n+1}x_n + ux_{n+1}}{uu_{n+1}}\end{aligned}$$

So by letting $v := u_1u_2 \dots u_nu_{n+1} = uu_{n+1}$ and $\widehat{v}_i := v/u_i \in U$ we see that the $\widehat{v}_i$ appear as the coefficients of the x_i again, e.g. we have $\widehat{v}_1 = \widehat{u}_1u_{n+1}$ and $\widehat{v}_{n+1} = u$. Hence we have just proved the induction step, that is $x_1/u_1 + x_2/u_2 + \dots + x_{n+1}/u_{n+1} = (\widehat{v}_1x_1 + \widehat{v}_2x_2 + \dots + \widehat{v}_{n+1}x_{n+1})/v$. □

Proof of (3.124):

(i) Let us first check the homomorphism property of κ: Clearly κ commutes with the addition so we only have to check that is also commutes with the scalar multiplication. By definition $\kappa : (a/u)x \mapsto ((a/u)x)/1$, but $((a/u)x)/1 = ((a/1)x)/u$ as by construction of the scalar multiplication on M_R we have $u(a/u)x = (u/1)(a/u)x = (ua/u)x = (a/1)x$. Now $((a/u)x)/1 = ((a/1)x)/u = (ax/u) = (a/u)(x/1)$ completes the S-linearity.

The surjectivity of κ is a special case of this: Given any $x/u \in U^{-1}M_R$ we get (using $a = 1$) $\kappa((1/u)x) = ((1/1)x)/u = x/u$. And then we also find the injectivity of κ, as $x/1 = 0/1$ means $wx = 0 \in M$ for some $w \in U$ and therefore $0 = (1/w)(wx) = (1/1)x = x$.

(ii) The R-linearity of λ_u is clear and as $\lambda_u(x) = ux = 0$ implies $0 = (1/u)(ux) = (u/u)x = (1/1)x = x$ we see that λ_u also in injective. And as $\lambda_u((1/u)x) = u(1/u)x = (u/u)x = (1/1)x = x$ it is surjective, as well.

(iii) If $\varphi : M \to N$ is S-linear then it also is R-linear, as in general we find $\varphi(ax) = \varphi((a/1)x) = (a/1)\varphi(x) = a\varphi(x)$. For the converse implication we will need $U/1 \subseteq \text{NZD}(N)$. Let us compute

$$\begin{aligned}\frac{u}{1}\varphi\left(\frac{a}{u}x\right) &= u\varphi\left(\frac{a}{u}x\right) = \varphi\left(u\frac{a}{u}x\right) = \varphi\left(\frac{ua}{u}x\right) \\ &= \varphi\left(\frac{a}{1}x\right) = \varphi(ax) = a\varphi(x) = \frac{a}{1}\varphi(x) \\ &= \frac{u}{1}\frac{a}{u}\varphi(x) = \frac{u}{1}\left(\frac{a}{u}\varphi(x)\right)\end{aligned}$$

That is we have $(u/1)y = 0$ for $y = \varphi((a/u)x) - (a/u)\varphi(x) \in N$. But as $u/1 \in \text{NZD}(N)$ this means $y = 0$ and hence $\varphi((a/u)x) = (a/u)\varphi(x)$, which is the S-linearity of φ.

□

Proof of (3.125):

(ii) It is quite easy to see that $U^{-1}\varphi$ is well-defined: if $x/u = y/v$ then there is some $w \in U$ such that $wvx = wuy$ such that $wv\varphi(x) = \varphi(wvx) = \varphi(wuy) = wu\varphi(y)$ which again implies $\varphi(x)/u = \varphi(y)/v$. Also it is easy to see, that $U^{-1}\varphi$ is a homomorphism of R-modules again

$$\begin{aligned} U^{-1}\varphi\left(a\frac{x}{u} + \frac{y}{u}\right) &= U^{-1}\varphi\left(\frac{ax+y}{u}\right) = \frac{\varphi(ax+y)}{u} \\ &= \frac{a\varphi(x)+\varphi(y)}{u} = a\frac{x}{u} + \frac{y}{u} \\ &= a\,U^{-1}\varphi\left(\frac{x}{u}\right) + U^{-1}\varphi\left(\frac{y}{u}\right) \end{aligned}$$

So it remains to verify the identities of the kernel and image of $U^{-1}\varphi$. First of all, for any $u \in U$ and any $x \in M$ we have $U^{-1}\varphi(x/u) = \varphi(x)/u \in U^{-1}(\mathrm{im}(\varphi))$. And conversely if $y/u \in U^{-1}(\mathrm{im}(\varphi))$ then there are some $v \in U$ and $x \in M$ such that $y/v = \varphi(x)/u$. That is $y/v = U^{-1}\varphi(x/u) \in \mathrm{im}(U^{-1}\varphi)$. Altogether we have

$$\mathrm{im}\left(U^{-1}\varphi\right) = U^{-1}\mathrm{im}(\varphi)$$

Also $x/u \in U^{-1}\mathrm{kn}(\varphi)$ this means that there are some $v \in U$ and $k \in \mathrm{kn}(\varphi)$ such that $x/u = k/v$. Therefore $U^{-1}\varphi(x/u) = U^{-1}\varphi(k/v) = \varphi(k)/v = 0/v = 0/1 = 0$ such that $x/u \in \mathrm{kn}(U^{-1}\varphi)$ again. And conversely for any $u \in U$ and any $x \in M$ we have $x/u \in \mathrm{kn}(U^{-1}\varphi)$ if and only if $0/1 = U^{-1}\varphi(x/u) = \varphi(x)/u$, which is $0 = w\varphi(x) = \varphi(wx)$ again, for some $w \in U$. That is $k := wx \in \mathrm{kn}(\varphi)$, so letting $v := wu$ we get $x/u = wx/wu = k/v \in U^{-1}\mathrm{kn}(\varphi)$. Altogether we also have

$$\mathrm{kn}\left(U^{-1}\varphi\right) = U^{-1}\mathrm{kn}(\varphi)$$

(i) We have already seen that $U^{-1}P$ is an R-module. And as $P \subseteq M$ we may regard the following map

$$U^{-1}P \hookrightarrow U^{-1}M \,:\, \frac{x}{u} \mapsto \frac{x}{u}$$

Note that this truly is a map, as the equivalence class of (u,x) has changed from a subset of $U \times P$ to a subset of $U \times M$. However it is obvious, that this map is both well-defined and injective as $(u,x) \sim (v,y)$ is the same in $U \times P$ and $U \times M$. Hence $U^{-1}P$ can be identified by its image under this embedding

$$U^{-1}P \cong_{\mathrm{m}} \left\{ \frac{x}{u} \mid x \in P, u \in U \right\}$$

So in the following we will regard $U^{-1}P' \subseteq U^{-1}M$ as a subset of $U^{-1}M$. Then we may take to the following map

$$\varrho \,:\, U^{-1}M \to U^{-1}(M/P) \,:\, \frac{x}{u} \mapsto \frac{x+P}{u}$$

First of all - using (ii) - ϱ is a well-defined $U^{-1}R$-module homomorphism, as it just is the localization of the canonical homomorphism $x \mapsto x + P$

$$\varrho = U^{-1}\left(M \to {}^{M}\big/_{P} : x \mapsto x + P\right)$$

Also the surjectivity of ϱ is trivial, as $x \in M$ and $u \in U$ can be chosen arbitrarily. And as

$x \mapsto x + P$ trivially has the kernel P we can also evaluate the kernel of ϱ by using (ii) again:

$$\mathsf{kn}(\varrho) \;=\; U^{-1}\mathsf{kn}(x \mapsto x + P) \;=\; U^{-1}P$$

Altogether, using the first isomorphism theorem (3.78.(ii)), ϱ induces the isomorphism of R-modules, that we claimed to exist

$$U^{-1}M \Big/ U^{-1}P \to U^{-1}(M/P) \;:\; \frac{x}{u} + U^{-1}P \mapsto \frac{x+P}{u}$$

(iii) Let us first check the well-definedness of the map given: if $(x_i/u_i) = (y_i/v_i)$ then (for any $i \in I$) there is some $w_i \in U$ such that $w_i v_i x_i = w_i u_i y_i$. Let us now define $w := \prod_{i\in\Omega} w_i$ and $\widehat{w}_i := w/w_i \in U$ as well. That is $w_i\widehat{w}_i = w$. Then multiplying this equation with $\widehat{u}_i\widehat{v}_i\widehat{w}_i$ we get

$$wv\widehat{u}_i x_i \;=\; \widehat{u}_i\widehat{v}_i\widehat{w}_i w_i v_i x_i \;=\; \widehat{u}_i\widehat{v}_i\widehat{w}_i w_i u_i y_i \;=\; wu\widehat{v}_i y_i$$

Composing these equalities for all $i \in I$ we found $wv(\widehat{u}_i x_i) = wu(\widehat{v}_i y_i)$ which yields $(\widehat{u}_i x_i)/u = (\widehat{v}_i y_i)/v$ again. Also it is clear, that $(\widehat{u}_i x_i)$ is contained in the direct *sum* of the M_i because $\widehat{u}_i x_i \neq 0$ disallows $wx_i = 0$ for some $w \in U$ which is $x_i/u_i \neq 0/1$ such that $i \in \Omega$. And the set Ω has been finite by the assumption that (x_i/u_i) comes from the direct *sum* of the $U^{-1}M_i$.

To prove the properties of an $U^{-1}R$-module homomorphism we let $n := \#\Omega$. Then for any $a/v \in U^{-1}R$ we may compute

$$\frac{a}{v}\left(\frac{x_i}{u_i}\right) \;=\; \left(\frac{ax_i}{vu_i}\right) \;\mapsto\; \frac{(\widehat{u}_i v^{n-1} a x_i)}{v^n u} \;=\; \frac{v^{n-1}a(\widehat{u}_i x_i)}{v^n u} \;=\; \frac{a}{v}\frac{(\widehat{u}_i x_i)}{u}$$

$$\left(\frac{x_i}{u_i}\right) + \left(\frac{y_i}{v_i}\right) \;=\; \left(\frac{v_i x_i + u_i y_i}{u_i v_i}\right) \;\mapsto\; \frac{(\widehat{u}_i\widehat{v}_i(v_i x_i + u_i y_i))}{uv}$$

Now we use $\widehat{u}_i u_i = 0$ and $\widehat{v}_i v_i = v$ again to continue with the computation $\widehat{u}_i\widehat{v}_i(v_i x_i + u_i y_i) = v\widehat{u}_i x_i + u\widehat{v}_i y_i$, which ultimately leads to

$$\left(\frac{x_i}{u_i}\right) + \left(\frac{y_i}{v_i}\right) \;\mapsto\; \frac{(v\widehat{u}_i x_i + u\widehat{v}_i y_i)}{uv} \;=\; \frac{(\widehat{u}_i x_i)}{u} + \frac{(\widehat{v}_i y_i)}{v}$$

Next we prove the injectivity of the homomorphism: suppose we have $(\widehat{u}_i x_i)/u = (\widehat{v}_i y_i)/v$ that is $wv(\widehat{u}_i x_i) = wu(\widehat{v}_i y_i)$ for some $w \in U$. That is for any $i \in I$ we have

$$wv\widehat{u}_i x_i \;\; = wu\widehat{v}_i y_i$$

Let us now define $w_i := \widehat{u}_i\widehat{v}_i w \in U$, then the above equation turns into $w_i v_i x_i = w_i u_i y_i$ which is $x_i/u_i = y_i/v_i$. And as $i \in I$ has been arbitrary this is $(x_i/u_i) = (y_i/v_i)$ again. It remains to prove the surjectivity of the homomorphism: thus consider any $(y_i)/v$ where $y_i \in M_i$. Then we let $x_i := y_i$ and $\Omega := \{\, i \in I \mid y_i \neq 0 \,\}$. If $i \in \Omega$ we take $u_i := v \in U$, else $u_i := 1 \in U$. Again we let $n := \#\Omega$ (which is finite) then $u = v^n$ and $\widehat{u}_i = v^{n-1}$ for any $i \in \Omega$. Then we get

$$\left(\frac{x_i}{u_i}\right) \;\mapsto\; \frac{(\widehat{u}_i x_i)}{u} \;=\; \frac{(v^{n-1}x_i)}{v^n} \;=\; \frac{(x_i)}{v} \;=\; \frac{(y_i)}{v}$$

□

Proof of (3.127):

- We first have to check the well-definedness of $\bar{k}$, that is given an $U^{-1}R$-sub-module Z of $U^{-1}M$ we need to verify that $P := \bar{k}(Z)$ truly is an R-sub-module of M, thereby $P = \{ x \in M \mid x/1 \in Z \}$. To do this one might argue, that κ is an R-module homomorphism an $P = \kappa^{-1}(Z)$ is just the preimage of Z or one might turn to a straightforward computation: First of all we have $0 \in P$, since $0/1 = 0 \in Z$. Also if x and $y \in P$, that is $x/1$ and $y/1 \in Y$ then $(x+y)/1 = x/1 + y/1 \in Z$ and $(ax)/1 = (a/1)(x/1) \in Z$ such that $x+y$ and $ax \in P$ again.

- Next we check the well-definedness of k, that is given an R-sumbodule P of M we need to verify that $Z := k(P)$ truly is an $U^{-1}R$-sub-module of $U^{-1}M$,thereby $Z = \{ x/u \mid x \in P, u \in U \}$. It is clear that $0 = 0/1 \in Z$ since $0 \in P$ and considering x/u and $y/v \in Z$ and any $a/w \in U^{-1}R$ we also get $x/u + y/v = (vx+uy)/uv \in Z$ since $vx + uy \in P$ and $(a/w)(x/u) = ax/uw \in Z$ since $ax \in P$ and $uw \in U$ again.

- So let us now check $k\bar{k} = \mathbb{1}$, that is for any $U^{-1}R$-sub-module Z of $U^{-1}M$ we get $k\bar{k}(Z) = Z$. To do this let $P := \bar{k}(Z)$, then by definition of k and $\bar{k}$ we get the following equality

$$k\bar{k}(Z) \;=\; \left\{ \frac{x}{u} \mid u \in U \text{ and } x \in P \right\} \;=\; \left\{ \frac{x}{u} \mid u \in U \text{ and } x/1 \in Z \right\}$$

 First consider $x/u \in k\bar{k}(Z)$, as we have seen this means $x/1 \in Z$. But as Z is an $U^{-1}R$-module, we hence get $x/u = (1/u)(x/1) \in Z$. Therefore we find the inclusion $k\bar{k}(Z) \subseteq Z$. Conversely if $x/u \in Z$, then $x/1 = (u/1)(x/u) \in Z$ as well, such that we also get $x/u \in k\bar{k}(Z)$.

- Consider any R-sub-module $P \leq_{\mathsf{m}} M$ then by definition of the maps k and $\bar{k}$ we get the following equality of sets

$$\begin{aligned}
\bar{k}k(P) &= \left\{ x \in M \mid x/1 \in \bar{k}(P) \right\} \\
&= \{ x \in M \mid \exists\, p \in P\ \exists\, u \in U : x/1 = p/u \} \\
&= \{ x \in M \mid \exists\, p \in P\ \exists\, u, w \in U : wux = wp \} \\
&= \{ x \in M \mid \exists\, v \in U : vx \in P \}
\end{aligned}$$

 Thereby the last equality can be seen in the following way: if $wux = wp$ then let $v := wu$, then $vx = wux = wp \in P$. Conversely if $vx \in P$ then let $p = vx$ and take $u = v$ and $w = 1$ then $wux = vx = p = wp$. In particular we get $P \subseteq \bar{k}k(P)$, as we may always take $v = 1$.

 Also suppose that $\bar{k}k(P) = P$ and consider some $x \in M$ and $u \in U$, with $ux \in P$. Then $x \in \bar{k}k(P)$ and hence $x \in P$. Conversely suppose, we have $ux \in P \implies x \in P$ for any $x \in M$ and $u \in U$. If now $x \in \bar{k}k(P)$ then $vx \in P$ for some $v \in U$. And by assumption this implies $x \in P$. That is $\bar{k}k(P) \subseteq P$ and as the converse inclusion is generally true this is $\bar{k}k(P) = P$.

- If P and $Q \leq_{\mathsf{m}} M$ are any two R-sub-modules of M, then $P \subseteq Q$ clearly implies $k(P) \subseteq k(Q)$, as stated in the claim. And in order to show $k(P \cap Q) = k(P) \cap k(Q)$ we need to verify the following

equality

$$\left\{ \frac{z}{w} \;\middle|\; \begin{array}{l} w \in U \\ z \in P \cap Q \end{array} \right\} = \left\{ \frac{x}{u} \;\middle|\; \begin{array}{l} u \in U \\ x \in P \end{array} \right\} \cap \left\{ \frac{y}{v} \;\middle|\; \begin{array}{l} v \in U \\ y \in Q \end{array} \right\}$$

The inclusion "$\subseteq$" is trivial, just let $x = z$ and $u = w$ respectively $y = z$ and $v = w$. Conversely suppose we are given some $x/u = y/v$ such that $x \in P$ and $y \in Q$. That is $z := avx = auy$ for some $a \in U$. Yet as P and Q are R-sub-modules, this implies $z \in P \cap Q$. And letting $w := auv$ we hence get $z/w \in k(P \cap Q)$. Now compute $z/w = avx/auv = x/u$ and $z/w = auy/auv = y/v$, from this we see $x/u = y/v = z/w \in k(P \cap Q)$.

- From the definition of $\bar{k}$ it is also clear, that $\bar{k}$ preserves inclusions, as stated in the claim. Also if Z_i (where $i \in I$) is a family of $U^{-1}R$-sub-modules of $U^{-1}M$, then it is clear that

$$\begin{aligned} \bar{k}\left(\bigcap_{i\in I} Z_i\right) &= \left\{ x \in M \;\middle|\; \frac{x}{1} \in \bigcap_{i\in I} Z_i \right\} \\ &= \left\{ x \in M \mid \forall\, i \in I : \frac{x}{1} \in Z_i \right\} \\ &= \bigcap_{i\in I} \left\{ x \in M \mid \frac{x}{1} \in Z_i \right\} = \bigcap_{i\in I} \bar{k}(Z_i) \end{aligned}$$

- At last we have to verify, that for any subset $X \subseteq M$ the sub-module of $U^{-1}M$ generated by $k(X)$ and the image $k(P)$ of the sub-module P of M generated by X are equal. To do this we first take a closer look at the sets involved - by definition we have

$$\begin{aligned} k\Big(\mathrm{Lh}_R(X)\Big) &= \left\{ \frac{1}{w} \sum_{i=1}^{n} a_i x_i \;\middle|\; w \in U, a_i \in R, x_i \in X \right\} \\ \mathrm{Lh}_{U^{-1}R}\Big(k(X)\Big) &= \left\{ \sum_{i=1}^{n} \frac{b_i}{v_i} \frac{x_i}{u_i} \;\middle|\; b_i \in R, u_i, v_i \in U, x_i \in X \right\} \end{aligned}$$

If $x = (1/w)\sum_i a_i x_i = \sum_i (a_i/w)(x_i/1)$ then it is clear that x is contained in the sub-module generated by $k(X)$. Conversely suppose we are given some $x = \sum_i (b_i/v_i)(x_i/u_i)$, then we define $u := u_1 \cdot \ldots u_n$ and $v := v_1 \cdot \cdots \cdot v_n$ also $\widehat{u}_i := u/u_i \in U$ and $\widehat{v}_i := v/v_i \in U$. If we now take to $w := uv$ and $a_i := \widehat{u}_i \widehat{v}_i b_i \in R$, then we can easily compute

$$\frac{1}{w}\sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n} \frac{a_i x_i}{w} = \sum_{i=1}^{n} \frac{\widehat{u}_i \widehat{v}_i b_i x_i}{uv} = \sum_{i=1}^{n} \frac{b_i x_i}{u_i v_i} \in \mathrm{Lh}_{U^{-1}R}\Big(k(X)\Big)$$

□

Proof of (2.133):

Two of the three implications are clear, thus we are only concerned with: if for any maximal ideal $\mathfrak{m} \trianglelefteq_{\mathrm{i}} R$ we have $a/1 = b/1 \in R_{\mathfrak{m}}$ then already $a = b \in R$. But since $a/1 = b/1$ is equivalent to $(a-b)/1 = 0/1$ it suffices

$$\forall\ \mathfrak{m}\ :\ \frac{a}{1} = \frac{0}{1} \in R_{\mathfrak{m}} \implies a = 0$$

By definition $a/1 = 0/1$ means that there is some $u \notin \mathfrak{m}$ such that $ua = 0$. And the latter can again be

formulated as $u \in \operatorname{ann}(a)$. Thus we have

$$\forall\ \mathfrak{m}\ :\ \operatorname{ann}(a)\ \not\subseteq\ \mathfrak{m}$$

Hence there is no maximal ideal $\mathfrak{m}$ containing $\operatorname{ann}(a)$. But as the annihilator $\operatorname{ann}(a)$ is an ideal this is only possible if $\operatorname{ann}(a) = R$ andchence $a = 1 \cdot a = 0$.
In the second claim it is clear that for any prime ideal $\mathfrak{p} \trianglelefteq_{\mathfrak{i}} R$ we get $R \subseteq R_{\mathfrak{p}} \subseteq F := \operatorname{quot}(R)$. Hence it is clear that $R \subseteq \bigcap_{\mathfrak{p}} R_{\mathfrak{p}}$. And as $\operatorname{Smax}(R) \subseteq \operatorname{Spec}(R)$ it also is clear that $\bigcap_{\mathfrak{p}} R_{\mathfrak{p}} \subseteq \bigcap_{\mathfrak{m}} R_{\mathfrak{m}}$ such that we only have to verify $\bigcap_{\mathfrak{m}} R_{\mathfrak{m}} \subseteq R$. Thus consider any $a/b \in F$ with $a/b \in \bigcap_{\mathfrak{m}} R_{\mathfrak{m}}$. That is for any maximal ideal $\mathfrak{m} \trianglelefteq_{\mathfrak{i}} R$ there are some $a(\mathfrak{m}) \in R$ and $b(\mathfrak{m}) \notin \mathfrak{m}$ such that $a/b = a(\mathfrak{m})/b(\mathfrak{m})$. Now define the ideal

$$\mathfrak{b}\ :=\ \langle b(\mathfrak{m}) \mid \mathfrak{m} \in \operatorname{Smax}(R)\rangle_{\mathfrak{i}}\quad \trianglelefteq_{\mathfrak{i}}\quad R$$

Suppose we had $\mathfrak{b} \neq R$, then there would be some maximal ideal $\mathfrak{m}$ such that $\mathfrak{m} \subseteq \mathfrak{m}$. But clearly $b(\mathfrak{m}) \in \mathfrak{b}$ although $b(\mathfrak{m}) \notin \mathfrak{m}$, a contradiction. That is $\mathfrak{b} = R$ and hence $1 \in \mathfrak{b}$. That is there is a finite subset $M \subseteq \operatorname{Smax}(R)$ and there are $r(\mathfrak{m}) \in R$ (where $\mathfrak{m} \in M$) such that $1 = \sum_{\mathfrak{m}} r(\mathfrak{m})b(\mathfrak{m})$. Now recall that $a/b = a(\mathfrak{m})/b(\mathfrak{m})$, then we find $a/b \in R$ by virtue of

$$\frac{a}{b}\ =\ 1 \cdot \frac{a}{b}\ =\ \left(\sum_{\mathfrak{m}\in M} r(\mathfrak{m})b(\mathfrak{m})\right)\frac{a}{b}\ =\ \sum_{\mathfrak{m}\in M} r(\mathfrak{m})a(\mathfrak{m})\ \in\ R$$

□

Proof of (2.119):

- As φ is a homomorphsim of rings, we have $1_S = \varphi(1_R) \in \varphi(U)$. If now $\varphi(u)$, $\varphi(v)$ are any two elements of $\varphi(U)$, then $\varphi(u)\varphi(v) = \varphi(uv) \in \varphi(U)$, since U is a multiplicatively closed set and thereby $uv \in U$ again. Together we see, that $\varphi(U)$ is multiplicatively closed, again.

- To prove that $U^{-1}\varphi$ is well-defined, we start with some $a/u = b/v \in U^{-1}R$. By definition that is $wva = wub$ for some $w \in U$ and hence $\varphi(wva) = \varphi(wub)$. That is $\varphi(w)\varphi(v)\varphi(a) = \varphi(w)\varphi(u)\varphi(b)$ and thereby $\varphi(a)/\varphi(u) = \varphi(b)/\varphi(v)$, as $\varphi(w) \in \varphi(U)$. As these are the images of a/u and b/v respectively, this is the well-definedness of $U^{-1}\varphi$.

- It is straightforward to check, that the map $U^{-1}\varphi$ inherits being a homomorphism of rings from φ. First of all $U^{-1}\varphi(1_R/1_R) = \varphi(1_R)/\varphi(1_R) = 1_S/1_S$. And for any a, $b \in R$ and u, $v \in U$ we compute

$$\begin{aligned}
U^{-1}\varphi\left(\frac{a}{u}\cdot\frac{b}{v}\right) &= U^{-1}\varphi\left(\frac{ab}{uv}\right) = \frac{\varphi(ab)}{\varphi(uv)} = \frac{\varphi(a)\varphi(b)}{\varphi(u)\varphi(v)} = \frac{\varphi(a)}{\varphi(u)}\cdot\frac{\varphi(b)}{\varphi(v)}\\
U^{-1}\varphi\left(\frac{a}{u}+\frac{b}{v}\right) &= U^{-1}\varphi\left(\frac{av+bu}{uv}\right) = \frac{\varphi(av+bu)}{\varphi(uv)}\\
&= \frac{\varphi(a)\varphi(v)+\varphi(b)\varphi(u)}{\varphi(u)\varphi(v)} = \frac{\varphi(a)}{\varphi(u)}+\frac{\varphi(b)}{\varphi(v)}
\end{aligned}$$

- If φ is injective, we just pursue the above arguments in reverse order: If $\varphi(a)/\varphi(u) = \varphi(b)/\varphi(v)$, then $\varphi(w)\varphi(v)\varphi(a) = \varphi(w)\varphi(u)\varphi(b)$ for some $w \in U$. But this is $\varphi(wva) = \varphi(wub)$ and as φ is injective, we conclude $wva = wub$ such that $a/u = b/v$. Thus $U^{-1}\varphi$ is injective again. Now, if φ is

surjective, then for any $s \in S$ there is some $a \in R$, such that $\varphi(a) = s$ and thereby $a/u \mapsto s/\varphi(u)$. Thus $U^{-1}\varphi$ reaches any element of $\varphi(U)^{-1}S$, which means it is surjectve. And as bijective just means "injective and surjective", we also see that $U^{-1}\varphi$ is bijective, whenever φ is.

□

Proof of (2.120):
In the first part we will prove the existence of the induced homomorphism $\overline{\varphi}$. And of course we start with the well-definedness of $\overline{\varphi}$ as a mapping. Thus let us regard $a/u = b/v \in U^{-1}R$. That is there is some $w \in U$ such that $vwa = uwb$. And thereby we get $\varphi(a)\varphi(u)^{-1} = \varphi(b)\varphi(v)^{-1}$ from

$$\varphi(v)\varphi(w)\varphi(a) \;=\; \varphi(vwa) \;=\; \varphi(uwb) \;=\; \varphi(u)\varphi(w)\varphi(b)$$

Next we have to check that $\overline{\varphi}$ truly is a homomorphism of rings. To do this consider any a/u and $b/v \in U^{-1}R$ and compute

$$\begin{aligned}
\overline{\varphi}\left(\frac{a}{u}\cdot\frac{b}{v}\right) &= \overline{\varphi}\left(\frac{ab}{uv}\right) = \varphi(a)\varphi(b)\varphi(u)^{-1}\varphi(v)^{-1} \\
&= \Big(\varphi(a)\varphi(u)^{-1}\Big)\Big(\varphi(b)\varphi(v)^{-1}\Big) = \overline{\varphi}\left(\frac{a}{u}\right)\cdot\overline{\varphi}\left(\frac{b}{v}\right) \\
\overline{\varphi}\left(\frac{a}{u}+\frac{b}{v}\right) &= \overline{\varphi}\left(\frac{av+bu}{uv}\right) = \Big(\varphi(a)\varphi(v)+\varphi(b)\varphi(u)\Big)\varphi(u)^{-1}\varphi(v)^{-1} \\
&= \varphi(a)\varphi(u)^{-1}+\varphi(b)\varphi(v)^{-1} = \overline{\varphi}\left(\frac{a}{u}\right)+\overline{\varphi}\left(\frac{b}{v}\right)
\end{aligned}$$

So we have proved the existence of the homomorphism $\overline{\varphi}$. It remains to verify that this is the unique homomorphism such that $\overline{\varphi}\kappa = \varphi$. That is we consider some homomorphism $\psi : U^{-1}R \to S$ such that for any $a \in R$ we get $\psi(a/1) = \varphi(a)$. Then for any $u \in U \subseteq R$ we get

$$\psi\left(\frac{1}{u}\right) \;=\; \psi\left(\left(\frac{u}{1}\right)^{-1}\right) \;=\; \psi\left(\frac{u}{1}\right)^{-1} \;=\; \varphi(u)^{-1}$$

And thereby we find for any $a/u \in U^{-1}R$ that $\psi(a/u) = \psi(a/1 \cdot 1/u) = \psi(a/1)\psi(1/u) = \varphi(a)\varphi(u)^{-1} = \overline{\varphi}$. That is $\psi = \overline{\varphi}$, that is $\overline{\varphi}$ is unique. □

Proof of (3.132):
As $\alpha : R \to S$ is a ring-homomorphism, it is clear that N can be turned into an R-module, keeping the addition of N and taking to the scalar multiplication $ay := \alpha(a)y$. And as $\alpha(U) \subseteq S^*$ the universal property (2.120) of the localization of rings yields a ring homomorphism $\overline{\alpha} : U^{-1}R \to S$ by letting

$$\overline{\alpha} \;:\; U^{-1}R \to S \;:\; \frac{a}{u} \mapsto \alpha(u)^{-1}\alpha(a)$$

In complete analogy we can turn N into an $U^{-1}R$-module, as well. This time we have to use the scalar multiplication $(a/u)y := \overline{\alpha}(a/u)y = \alpha(u)^{-1}\alpha(a)y$ (and keep the additon of N again).

Next we prove, that $\overline{\varphi}$ truly is a well-defined homomorphism of $U^{-1}R$ modules. Thus consider $x/u = y/v \in U^{-1}M$, that is there is some $w \in U$ such that $wvx = wuy$. In particular (since φ is R-linear) we

get

$$\begin{aligned}\alpha(w)\alpha(u)\varphi(x) &= \alpha(wu)\varphi(x) = wu\varphi(x) = \varphi(wux)\\ &= \varphi(wuy) = wu\varphi(y) = \alpha(wu)\varphi(y) = \alpha(w)\alpha(v)\varphi(y)\end{aligned}$$

And as $\alpha(w) \in S^*$ is invertible, this implies $\alpha(u)\varphi(x) = \alpha(v)\varphi(y)$. Again this is $\overline{\varphi}(x/u) = \alpha(u)^{-1}\varphi(x) = \alpha(v)^{-1}\varphi(y) = \overline{\varphi}(y/v)$. Hence $\overline{\varphi}$ is well-defined and we have to check the homomorphism properties: consider $a/u \in U^{-1}R$ and x/u, $y/v \in U^{-1}M$ again, then we simply compute

$$\begin{aligned}\overline{\varphi}\left(\frac{x}{u}+\frac{y}{v}\right) &= \overline{\varphi}\left(\frac{vx+uy}{uv}\right) = \alpha(uv)^{-1}\varphi(vx+uy)\\ &= \alpha(u)^{-1}\alpha(v)^{-1}\Big(v\varphi(x)+u\varphi(y)\Big)\\ &= \alpha(u)^{-1}\varphi(x)+\alpha(v)^{-1}\varphi(y)\end{aligned}$$

where the latter equality holds true, as $v\varphi(x) = \alpha(v)\varphi(x)$ and $u\varphi(y) = \alpha(u)\varphi(y)$ by definition of the scalar multiplication on N. Likewise

$$\begin{aligned}\overline{\varphi}\left(\frac{a}{u}\frac{y}{v}\right) &= \overline{\varphi}\left(\frac{ay}{uv}\right) = \alpha(uv)^{-1}\varphi(ay)\\ &= \alpha(u)^{-1}\alpha(v)^{-1}\alpha(a)\varphi(y) = \frac{a}{u}\,\overline{\varphi}\left(\frac{y}{v}\right)\end{aligned}$$

It remains to verify the uniqueness of this homomorphism. Hence suppose $\psi : U^{-1}M \to N$ is any homomorphism of R-modules, such that $\varphi = \psi\kappa$. That is $\varphi(x) = \psi(x/1)$ for any $x \in M$. Then for any $u \in U$ we also get $\varphi(x) = \psi(x/1) = \psi(ux/u) = u\psi(x/u) = \alpha(u)\psi(x/u)$. Now, as $\alpha(u) \in S^*$ again we hence get $\psi(x/u) = \alpha(u)^{-1}\varphi(x) = \overline{\varphi}(x/u)$. □

Proof of (2.122):

- By definition $\kappa^{-1}(\mathfrak{u})$ is the set of all $a \in R$ such that $a/1 = \kappa(a) \in \mathfrak{u}$, and this has already been the first claim. And $\kappa^{-1}(\mathfrak{a})$ is an ideal of R by virtue of (1.76.(vii)).

- " $\supseteq$ " If $a \in \mathfrak{a}$ then $a/1 = \kappa(a) \in \kappa(\mathfrak{a}) \subseteq U^{-1}\mathfrak{a}$. And for any $u \in U$ we hence also get $a/u = (1/u)(a/1) \in U^{-1}\mathfrak{a}$. "$\subseteq$" Conversely consider any $x \in \langle\kappa(\mathfrak{a})\rangle_{\mathfrak{i}}$. I.e. there are $a_i \in \mathfrak{a}$ and $x_i = b_i/v_i \in U^{-1}R$ such that

 $$x = \sum_{i=1}^{n} x_i\kappa(a_i) = \sum_{i=1}^{n}\frac{a_ib_i}{v_i}$$

 We now let $v := v_1 \ldots v_n \in U$ and $\widehat{v}_i := v/v_i \in U$ then a straightforward computation shows $x = a/v$ for some $a := \sum_i a_ib_i\widehat{v}_i \in \mathfrak{a}$

 $$x = \sum_{i=1}^{n}\frac{a_ib_i}{v_i} = \sum_{i=1}^{n}\frac{a_ib_i\widehat{v}_i}{v} = \frac{a}{v}$$

□

Proof of (2.124):

- First of all $\mathfrak{a} : U$ is an ideal - $0 \in \mathfrak{a} : U$ since $0 = 1 \cdot 0 \in \mathfrak{a}$. Now consider $a, b \in \mathfrak{a} : U$. That is there are some $u, v \in V$ such that ua and $vb \in \mathfrak{a}$. This yields $uv(a+b) = v(ua) + u(vb) \in \mathfrak{a}$ and hence $a + b \in \mathfrak{a} : U$. Likewise for any $r \in R$ we get $u(ra) = r(ua) \in \mathfrak{a}$ and hence $ra \in \mathfrak{a} : U$.

- Next it is clear that $\mathfrak{a} \subseteq \mathfrak{a} : U$, because if $a \in \mathfrak{a}$ then $a = 1 \cdot a \in \mathfrak{a}$ (due to $1 \in U$) and hence $a \in \mathfrak{a} : U$.

- We finally wish to prove $(U^{-1}\mathfrak{a}) \cap R = \mathfrak{a} : U$. Consider any $b \in \mathfrak{a} : U$, that is $vb \in \mathfrak{a}$ for some $v \in U$. Then $b/1 = vb/v \in U^{-1}\mathfrak{a}$ and hence $b \in (U^{-1}\mathfrak{a}) \cap R$. Conversely let $b \in (U^{-1}\mathfrak{a}) \cap R$, by definition this means $b/1 \in U^{-1}\mathfrak{a}$. That is there is some $a \in \mathfrak{a}$, $u \in U$ such that $b/1 = a/u$. That is there is some $v \in U$ such that $uvb = va \in \mathfrak{a}$. And as $uv \in U$ this means $b \in \mathfrak{a} : U$.

□

Proof of (2.125):

- $U^{-1}(\mathfrak{a} \cap \mathfrak{b}) = (U^{-1}\mathfrak{a}) \cap (U^{-1}\mathfrak{b})$: if $x \in U^{-1}(\mathfrak{a} \cap \mathfrak{b})$ then by definition there are some $a \in \mathfrak{a} \cap \mathfrak{b}$ and $u \in U$ such that $x = a/u$. But as $a \in \mathfrak{a}$ and $a \in \mathfrak{b}$ this already means $x \in U^{-1}\mathfrak{a}$ and $x \in U^{-1}\mathfrak{b}$. If conversely $x = a/u \in U^{-1}\mathfrak{a}$ and $x = b/v \in U^{-1}\mathfrak{b}$ then $a/u = b/v$ means that there is some $w \in U$ such that $vwa = uwb \in \mathfrak{a} \cap \mathfrak{b}$. Hence $x = (vwa)/(uvw) = (uwb)/(uvw) \in U^{-1}(\mathfrak{a} \cap \mathfrak{b})$.

- $U^{-1}(\mathfrak{a} + \mathfrak{b}) = (U^{-1}\mathfrak{a}) + (U^{-1}\mathfrak{b})$: if $x \in U^{-1}(\mathfrak{a} + \mathfrak{b})$ then there are some $a \in \mathfrak{a}$, $b \in \mathfrak{b}$ and $u \in U$ such that $x = (a+b)/u = (a/u) + (b/u) \in (U^{-1}\mathfrak{a}) + (U^{-1}\mathfrak{b})$. And if we are conversely given any $a/u \in U^{-1}\mathfrak{a}$ and $b/v \in U^{-1}\mathfrak{b}$ then $a/u + b/v = (au + bv)/(uv) \in U^{-1}(\mathfrak{a} + \mathfrak{b})$.

- $U^{-1}(\mathfrak{a}\,\mathfrak{b}) = (U^{-1}\mathfrak{a})\,(U^{-1}\mathfrak{b})$: if $x \in U^{-1}(\mathfrak{a}\,\mathfrak{b})$ then there are some $f \in \mathfrak{a}\,\mathfrak{b}$ and $u \in U$ such that $x = f/u$. Again f is of the form $f = \sum_i a_i b_i$ for some $a_i \in \mathfrak{a}$ and $b_i \in \mathfrak{b}$. Altogether we get

$$x \;=\; \frac{f}{u} \;=\; \sum_{i=1}^{n} \frac{a_i b_i}{u} \;=\; \sum_{i=1}^{n} \frac{a_i}{1}\frac{b_i}{u} \;\in\; (U^{-1}\mathfrak{a})\,(U^{-1}\mathfrak{b})$$

 Conversely consider $a_i/u_i \in U^{-1}\mathfrak{a}$ and $b_i/v_i \in U^{-1}\mathfrak{b}$. As always we let $u := u_1 \dots u_n$ and $\widehat{u}_i := u/u_i \in U$ again, likewise $v := v_1 \dots v_n$ and $\widehat{v}_i := v/v_i \in U$. Then $a_i/u_i = (a_i\widehat{u}_i)/u$, $b_i/v_i = (b_i\widehat{v}_i)/v$ and

$$\sum_{i=1}^{n} \frac{a_i}{u_i}\frac{b_i}{v_i} \;=\; \sum_{i=1}^{n} \frac{a_i\widehat{u}_i}{u}\frac{b_i\widehat{v}_i}{v} \;=\; \frac{1}{uv}\sum_{i=1}^{n} \widehat{u}_i a_i \widehat{v}_i a_i b_i \;\in\; U^{-1}\big(\mathfrak{a}\,\mathfrak{b}\big)$$

- $U^{-1}\sqrt{\mathfrak{a}} = \sqrt{U^{-1}\mathfrak{a}}$: if $x \in U^{-1}\sqrt{\mathfrak{a}}$ then $x = b/v$ for some $b \in \sqrt{\mathfrak{a}}$ and $v \in U$. That is there is some $k \in \mathbb{N}$ such that $b^k \in \mathfrak{a}$. And therefore $x^k = b^k/v^k \in U^{-1}\mathfrak{a}$. Hence x is contained in the radical of $U^{-1}\mathfrak{a}$. Conversely consider any $x = b/v$ such that there is some $k \in \mathbb{N}$ with $x^k = b^k/v^k \in U^{-1}\mathfrak{a}$. Then there is some $a \in \mathfrak{a}$ and $u \in U$ such that $b^k/v^k = a/u$. That is $uwb^k = v^k wa \in \mathfrak{a}$ for some $w \in U$. Hence $(uwb)^k = (uw)^{k-1}(uwb^k) \in \mathfrak{a}$, that is $uwb \in \sqrt{\mathfrak{a}}$. And this agian yields $x = b/v = (uwb)/(uvw) \in U^{-1}\sqrt{\mathfrak{a}}$.

- Next we prove $(\mathfrak{a} : U) : U = \mathfrak{a} : U$. Clearly, as $1 \in U$ we have $\mathfrak{a} : U \subseteq (\mathfrak{a} : U) : U$ (as for any $a \in \mathfrak{a} : U$ we have $a = a \cdot 1 \in (\mathfrak{a} : U) : U$). Conversely if $a \in (\mathfrak{a} : U) : U$ then there is some $u \in U$ such that $au \in \mathfrak{a} : U$. Again this means that there is some $v \in U$ such that $a(uv) = (au)v \in \mathfrak{a}$. But as $uv \in U$ this again yields $a \in \mathfrak{a} : U$.

- For $(\mathfrak{a} \cap \mathfrak{b}) : U = (\mathfrak{a} : U) \cap (\mathfrak{b} : U)$ we use a straightforward reasoning again: If $a \in (\mathfrak{a} \cap \mathfrak{b}) : U$ then there is some $u \in U$ such that $au \in \mathfrak{a} \cap \mathfrak{b}$. And this again means $a \in \mathfrak{a} : U$ *and* $a \in \mathfrak{b} : U$. Conversely consider $a \in (\mathfrak{a} : U) \cap (\mathfrak{b} : U)$. That is there are v, $w \in U$ such that $av \in \mathfrak{a}$ and $aw \in \mathfrak{b}$. Now let $u := vw \in U$ then $au = (av)w = (aw)v \in \mathfrak{a} \cap \mathfrak{b}$ such that $a \in (\mathfrak{a} \cap \mathfrak{b}) : U$.

- We turn our attention to $\sqrt{\mathfrak{a} : U} = \sqrt{\mathfrak{a}} : U$. If $\mathfrak{a} : U = R$ then we get $\sqrt{\mathfrak{a} : U} = \sqrt{R} = R$. And as $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$ we also have $R = \mathfrak{a} : U \subseteq \sqrt{\mathfrak{a}} : U \subseteq R$. And hence we get $\sqrt{\mathfrak{a} : U} = R = \sqrt{\mathfrak{a}} : U$. Thus assume $\mathfrak{a} : U \neq R$. If $x \in \sqrt{\mathfrak{a} : U}$ then by definition there is some $k \in \mathbb{N}$ such that $x^k \in \mathfrak{a} : U$. And this means $x^k u \in \mathfrak{a}$ for some $u \in U$. Clearly we have $k \geq 1$ as else $u \in \mathfrak{a}$ such that $\mathfrak{a} : U = R$. And thereby we get $(xu)^k = (x^k u)u^{k-1} \in \mathfrak{a}$, too. But this means $xu \in \sqrt{\mathfrak{a}}$ and hence $x \in \sqrt{\mathfrak{a}} : U$. Conversely if $x \in \sqrt{\mathfrak{a}} : U$ then there is some $u \in U$ such that $xu \in \sqrt{\mathfrak{a}}$. Thus there is some $k \in \mathbb{N}$ such that $x^k u^k = (xu)^k \in \mathfrak{a}$. But as $u^k \in U$ this yields $x^k \in \mathfrak{a} : U$ and hence $x \in \sqrt{\mathfrak{a} : U}$.

- $(\mathfrak{u} \cap \mathfrak{w}) \cap R = \kappa^{-1}(\mathfrak{u} \cap \mathfrak{w}) = \kappa^{-1}(\mathfrak{u}) \cap \kappa^{-1}(\mathfrak{w}) = (\mathfrak{u} \cap R) \cap (\mathfrak{w} \cap R) = \mathfrak{a} \cap \mathfrak{b}$.

- $(\mathfrak{u} + \mathfrak{w}) \cap R = (\mathfrak{a} + \mathfrak{b}) : U$: if $c \in (\mathfrak{a} + \mathfrak{b}) : U$ then there are some $a \in \mathfrak{a}$, $b \in \mathfrak{b}$ and $u \in U$ such that $uc = a + b$. That is $(uc)/1 = (a + b)/1 = (a/1) + (b/1) \in \mathfrak{u} + \mathfrak{w}$. And thereby also $c/1 = (1/u)((uc)/1) \in \mathfrak{u} + \mathfrak{w}$. But this finally is $c \in (\mathfrak{u} + \mathfrak{w}) \cap R$. Conversely let $c \in (\mathfrak{u} + \mathfrak{w}) \cap R$, that is $c/1 \in \mathfrak{u} + \mathfrak{w}$. Thereby we find $a/u \in \mathfrak{u}$ and $b/v \in \mathfrak{w}$ such that $c/1 = a/u + b/v = (va + ub)/uv$. Hence there is some $w \in U$ such that $uvwc = vwa + uwb \in \mathfrak{a} + \mathfrak{b}$ (as $a/u \in \mathfrak{u}$ implies $a/1 = (u/1)(a/u) \in \mathfrak{u}$ and hence $a \in \mathfrak{a}$, likewise $b \in \mathfrak{b}$). And as $uvw \in U$ this is $c \in (\mathfrak{a} + \mathfrak{b}) : U$.

- $(\mathfrak{u}\,\mathfrak{w}) \cap R = (\mathfrak{a}\,\mathfrak{b}) : U$: if $c \in (\mathfrak{a}\,\mathfrak{b}) : U$ then there are some $a_i \in \mathfrak{a}$, $b_i \in \mathfrak{b}$ and $u \in U$ such that $uc = \sum_i a_i b_i \in \mathfrak{a}\,\mathfrak{b}$. Thereby $(uc)/1 = \sum_i (a_i/1)(b_i/1) \in \mathfrak{u}\,\mathfrak{w}$ and hence $c/1 = (1/u)((uc)/1) \in \mathfrak{u}\,\mathfrak{w}$ which means $c \in (\mathfrak{u}\,\mathfrak{w}) \cap R$. And if conversely $c \in (\mathfrak{u}\,\mathfrak{w}) \cap R$ then there are $a_i/u_i \in \mathfrak{u}$ and $b_i/v_i \in \mathfrak{w}$ such that
$$\frac{c}{1} \;=\; \sum_{i=1}^{n} \frac{a_i}{u_i}\frac{b_i}{v_i} \;=\; \sum_{i=1}^{n} \frac{a_i b_i \widehat{u}_i \widehat{v}_i}{uv} \;\in\; \mathfrak{u}\,\mathfrak{w}$$
where as usual $u := u_1 \ldots u_n$, $v := v_1 \ldots v_n$ and $\widehat{u}_i := u/u_i$, $\widehat{v}_i := v/v_i \in U$. From this equality we again get $uvwc = \sum_i a_i b_i \widehat{u}_i \widehat{v}_i \in \mathfrak{a}\,\mathfrak{b}$ for some $w \in U$ (as $a_i/u_i \in \mathfrak{u}$ implies $a_i/1 = (u_i/1)(a_i/u_i) \in \mathfrak{u}$ and hence $a_i \in \mathfrak{a}$, likewise $b_i \in \mathfrak{b}$). And as $uvw \in U$ this is $c \in (\mathfrak{a}\,\mathfrak{b}) : U$.

- $\sqrt{\mathfrak{u}} \cap R = \sqrt{\mathfrak{a}}$: if $b \in \sqrt{\mathfrak{u}} \cap R$ then $b/1 \in \sqrt{\mathfrak{u}}$, that is there is some $k \in \mathbb{N}$ such that $(b/1)^k = b^k/1 \in \mathfrak{u}$. Again this is $b^k \in \mathfrak{u} \cap R = \mathfrak{a}$ and hence $b \in \sqrt{\mathfrak{a}}$. Conversely if $b \in \sqrt{\mathfrak{a}}$ then $b^k \in \mathfrak{a}$ for some $k \in \mathbb{N}$. Hence $(b/1)^k = b^k/1 \in \mathfrak{u}$ which yields $b/1 \in \sqrt{\mathfrak{u}}$ and thereby $b \in \sqrt{\mathfrak{u}} \cap R$.

□

Proof of (2.127):

- If x/u is contained in $U^{-1} \bigcap_i \mathfrak{a}_i$ then x is an element of the intersection $x \in \bigcap_i \mathfrak{a}_i$ and hence $x \in \mathfrak{a}_i$ for any $i \in I$. But this means $x/u \in U^{-1}\mathfrak{a}_i$ and as this is true for any $i \in I$, we get $x/u \in \bigcap_i U^{-1}\mathfrak{a}_i$.

- For the converse inclusion we assumed that any $\mathfrak{p}_i \trianglelefteq_{\mathfrak{i}} R$ is a prime ideal satisfying $\mathfrak{p}_i \cap U = \emptyset$. If now $x/u \in \bigcap_i U^{-1}\mathfrak{p}_i$ then for any $i \in I$ there are some $p_i \in \mathfrak{p}_i$ and $u_i \in U$ such that $x/u =$

$p_i/u_i \in U^{-1}\mathfrak{p}_i$. Now fix any $j \in I$ and let $p := p_j$. Regarding any $i \in I$ we then find

$$\frac{p}{u_j} \;=\; \frac{x}{u} \;=\; \frac{p_i}{u_i}$$

That is there is some $v_i \in U$ such that $v_i u_i p = v_i u_j p_i$. As $p_i \in \mathfrak{p}_i$ we have $v_i u_i p \in \mathfrak{p}_i$. But $\mathfrak{p}_i \cap U = \emptyset$ such that $v_i u_i \notin \mathfrak{p}_i$. As $\mathfrak{p}_i$ also is prime, we conclude $p \in \mathfrak{p}_i$. And as this is true for any $i \in I$. Therefore $x/u = p/u_j \in U^{-1}\bigcap_i \mathfrak{p}_i$ such that both sets are equal.

- The second identity is easy: Clearly $x \in \bigcap_i(\mathfrak{u}_i \cap R)$ is equivalent to $x \in \mathfrak{u}_i \cap R$ for any $i \in I$. But this is just $x/1 \in \mathfrak{u}_i$ for any $i \in I$. Hence this again is equivalent to $x/1 \in \bigcap_i \mathfrak{u}_i$ and this again is just another way of saying $x \in (\bigcap_i \mathfrak{u}_i) \cap R$.

□

Proof of (2.128):
Nearly all of the statements are purely definitional. The two exceptions to this are the equalities claimed for $U^{-1}\mathrm{Spec}(R)$ and $U^{-1}\mathrm{Smax}(R)$: Consider any prime ideal $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ with $\mathfrak{p} \cap U = \emptyset$. If now $ua \in \mathfrak{p}$ then $u \in \mathfrak{p}$ or $a \in \mathfrak{p}$, as $\mathfrak{p}$ is prime. But $u \in \mathfrak{p}$ is absurd, due to $\mathfrak{p} \cap U = \emptyset$. This only leaves $a \in \mathfrak{p}$ and hence $\mathfrak{p} \in U^{-1}\mathrm{Ideal}(R)$. Conversely let $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ be a prime ideal with $\mathfrak{p} = \mathfrak{p} : U$. If now $u \cdot 1 = u \in \mathfrak{p} \cap U$ then $1 \in \mathfrak{p} : U = \mathfrak{p}$ in contradiction to $\mathfrak{p} \neq R$. Hence we get $\mathfrak{p} \cap U = \emptyset$. Now recall that any maximal ideal is prime. Then repeating the arguments above we also find $\mathfrak{m} = \mathfrak{m} : U \iff \mathfrak{m} \cap U = \emptyset$ for any maximal ideal $\mathfrak{m} \trianglelefteq_{\mathrm{i}} R$. □

Proof of (2.129):

- First of all it is clear that the mapping $\mathfrak{u} \mapsto \mathfrak{u} \cap R = \kappa^{-1}(\mathfrak{u})$ maps ideals to ideals, as it is just the pull back along the homomorphism κ. Now suppose that $ua \in \mathfrak{u} \cap R$ - this is $ua/1 \in \mathfrak{u}$ and hence $a/1 = (1/u)(ua/1) \in \mathfrak{u}$. But this again implies $a \in \mathfrak{u} \cap R$ and hence $\mathfrak{u} \cap R \in U^{-1}\mathrm{Ideal}(R)$. Conversely for any ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ the set $U^{-1}\mathfrak{a}$ is an ideal of $U^{-1}R$ by (2.122). Thus both of the mappings are well-defined.

- Next we remark that for any $\mathfrak{a} \in U^{-1}\mathrm{Ideal}(R)$ and $\mathfrak{u} \trianglelefteq_{\mathrm{i}} U^{-1}R$ we obtain

$$(U^{-1}\mathfrak{a}) \cap R \;=\; \mathfrak{a} : U \;=\; \mathfrak{a}$$

$$U^{-1}(\mathfrak{u} \cap R) \;=\; \{\, a/u \mid a/1 \in \mathfrak{u}, u \in U \,\} \;=\; \mathfrak{u}$$

 Thereby the first equality follows from (2.124) and the definition of $U^{-1}\mathrm{Ideal}(R)$. And for the second equality consider a/u where $a/1 \in \mathfrak{u}$. Then we find that $a/u = (1/u)(a/1) \in \mathfrak{u}$ as well. And if conversely $a/u \in \mathfrak{u}$ then we likewise get $a/1 = (u/1)(a/u) \in \mathfrak{u}$ again. Altogether these equalities yield that the maps given are mutually inverse.

- If $\mathfrak{a} \subseteq \mathfrak{b}$ and we consider any $a/u \in U^{-1}\mathfrak{a}$ then $a \in \mathfrak{a} \subseteq \mathfrak{b}$ and hence $a/u \in U^{-1}\mathfrak{b}$. And if conversely $\mathfrak{u} \subseteq \mathfrak{w}$ and $a \in \mathfrak{u} \cap R$ then $a/1 \in \mathfrak{u} \subseteq \mathfrak{w}$ such that $a \in \mathfrak{w} \cap R$. That is both of the mappings are order preserving.

- Next we want to prove that this correspondence preserves radical ideals. Thus if $\mathfrak{a} \in U^{-1}\mathrm{Ideal}(R)$ is a radical ideal then we have $\mathfrak{a} = \sqrt{\mathfrak{a}}$ and thereby $U^{-1}\mathfrak{a}$ is a radical ideal due to (2.125) (see

below). Likewise we see that if $\mathfrak{u} \in \mathrm{Ideal}(U^{-1}R)$ is a radical ideal, then $\mathfrak{u} \cap R$ is radical, too:

$$\sqrt{U^{-1}\mathfrak{a}} \;=\; U^{-1}\big(\sqrt{\mathfrak{a}}\big) \;=\; U^{-1}\mathfrak{a}$$

$$\sqrt{\mathfrak{u} \cap R} \;=\; \sqrt{\mathfrak{u}} \cap R \;=\; \mathfrak{u} \cap R$$

- Thus it only remains to verify that prime (resp. maximal) ideals are truly correspond to prime (resp. maximal) ideals. For prime ideals this is an easy, straightforward computation: $ab/uv \in U^{-1}\mathfrak{p}$ implies $ab \in \mathfrak{p}$ thus $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$ which again is $a/u \in U^{-1}\mathfrak{p}$ or $b/v \in U^{-1}\mathfrak{p}$. Conversely $ab \in \mathfrak{r} \cap R$ implies $ab/1 \in \mathfrak{r}$ and hence $a/1 \in \mathfrak{r} \cap R$ or $b/1 \in \mathfrak{r} \cap R$. And for maximal ideals this is clear, as the mappings given obviously preserve inclusions.

□

Proof of (2.132):

(i) Consider any two polynomials $f, g \in R[t \mid A]$ and $u, v \in U$. Let us first evaluate what property (a) $f/u = g/v$ means explicitly: By definition of the localisation, this is $wvf = wug$ for some $w \in U$. And if we write out f and g as linear combinations over the monomials t^α this turns into

$$\begin{aligned}
\frac{f}{u} = \frac{g}{v} \quad &\Longleftrightarrow \quad \exists\, w \in U \,:\, wv \sum_{\alpha\in A} f[\alpha]t^\alpha \;=\; wu \sum_{\alpha\in A} g[\alpha]t^\alpha \\
&\Longleftrightarrow \quad \exists\, w \in U \,:\, \sum_{\alpha\in A} \big(wvf[\alpha] - wug[\alpha]\big)t^\alpha \;=\; 0 \\
&\Longleftrightarrow \quad \exists\, w \in U \,:\, \forall\, \alpha \in A \,:\, wvf[\alpha] \;=\; wug[\alpha]
\end{aligned}$$

On the other hand let us evaluate let us evaluate property (b) that the images of f/u and g/v are identical. Clearly that is $f[\alpha]/u = g[\alpha]/v$ for any $\alpha \in A$ and hence we find

$$\sum_{\alpha\in A} \frac{f[\alpha]}{u} t^\alpha \;=\; \sum_{\alpha\in A} \frac{g[\alpha]}{v} t^\alpha \quad\Longleftrightarrow\quad \forall\, \alpha \in A \,:\, \exists\, w(\alpha) \in U \,:\, w(\alpha)vf[\alpha] \;=\; w(\alpha)ug[\alpha]$$

In the direction (a) $\Longrightarrow$ (b) we may take $w(\alpha) := w$ and thus the map $f/u \mapsto \sum_\alpha f[\alpha]/u\, t^\alpha$ is well-defined. For (b) $\Longrightarrow$ (a) we use that $A_f := \{\, \alpha \in A \mid f[\alpha] \neq 0 \,\}$ is a finite set and the same is true for $A_g \subseteq A$. That is for any $\alpha \notin A_f \cup A_g$ we have $f[\alpha] = g[\alpha] = 0$. For such an α we may take $w(\alpha) = 1$ in this case. Therefore the following product in R in truth runs over the finite subset $A_f \cup A_g \subseteq A$ only and hence returns a well-defined element of U

$$w \;:=\; \prod_{\alpha\in A} w(\alpha) \;\in\; U$$

If we take $\widehat{w}(\alpha) := w/w(\alpha) \in U$, as usual we get $\widehat{w}(\alpha) \cdot w(\alpha) = w$ for any $\alpha \in A$. So multiplying the identity $w(\alpha)vf[\alpha] = w(\alpha)ug[\alpha]$ with $\widehat{w}(\alpha)$ we get $wvf[\alpha] = wug[\alpha]$ for any $\alpha \in A$. And as this w is identical for any $\alpha \in A$, we see (b) $\Longrightarrow$ (a), as well. This is the injectivity of the map $f/u \mapsto \sum_\alpha f[\alpha]/u\, t^\alpha$. And as this map is defined by linear expansion of $t^\alpha \mapsto 1/ut^\alpha$ it is clear, that it is R-linear again. It also is a homomorphism of rings, as the multiplications on the polynomial rings $R[t \mid A]$ and $U^{-1}R[t \mid A]$ have bee defined in precisely the same way.

So it only remains to verify the surjectivity: That is we are given any polynomial $p \in U^{-1}R[t \mid A]$

and need to find some $f \in R[t \mid A]$ and $u \in U$ such that $f/u \mapsto p$. By definition any coefficient of p is if the form $p[\alpha] = a[\alpha]/u[\alpha]$ for some $a[\alpha] \in R$ and $u[\alpha] \in U$. Again $A_p = \{\, \alpha \in A \mid p[\alpha] \neq 0 \,\}$ is finite and for $\alpha \notin A_p$ we may take $u[\alpha] = 1$, as $0/u = 0/1$ for any $u \in U$. Therefore the following product is a well-defined element of U again, as in truth it runs over A_p only

$$u \;:=\; \prod_{\alpha \in A} u[\alpha] \;\in\; U$$

As before, let $\widehat{u}[\alpha] := u/u[\alpha] \in U$ such that $\widehat{u}[\alpha] \cdot u[\alpha] = u$. Also let $f[\alpha] := \widehat{u}[\alpha]a[\alpha] \in R$, then it is easy to compute, that we have the following identity

$$p[\alpha] \;=\; \frac{a[\alpha]}{u[\alpha]} \;=\; \frac{a[\alpha]\widehat{u}[\alpha]}{u[\alpha]\widehat{u}[\alpha]} \;=\; \frac{f[\alpha]}{u}$$

Now define $f := \sum_\alpha f[\alpha]t^\alpha$ and note that $A_f = \{\, \alpha \in A \mid f[\alpha] \,\} \subseteq A_p$ is finite (such that f truly is a polynomial in $R[t \mid A]$), then it becomes apparent, that

$$\frac{f}{u} \;\mapsto\; \sum_{\alpha \in A} \frac{f[\alpha]}{u} t^\alpha \;=\; \sum_{\alpha \in A} p[\alpha]\, t^\alpha \;=\; p$$

(ii) Let us regard the map $b/v \mapsto (b+\mathfrak{a})/(v+\mathfrak{a})$. We first check its well-definedness: Suppose $a/u = b/v \in U^{-1}R$, that is there is some $w \in U$ such that $vwa = uwb$. Of course this yields $(v+\mathfrak{a})(w+\mathfrak{a})(a+\mathfrak{a}) = (u+\mathfrak{a})(w+\mathfrak{a})(b+\mathfrak{a})$. But as $w \in U$ we also have $w+\mathfrak{a} \in U/\mathfrak{a}$ and hence $(a+\mathfrak{a})/(u+\mathfrak{a}) = (b+\mathfrak{a})/(v+\mathfrak{a})$. And it is immediately clear that this map even is a homomorphism of rings. Next we will prove its surjectivity, that is we are given any $(b+\mathfrak{a})/(v+\mathfrak{a}) \in (U/\mathfrak{a})^{-1}(R/\mathfrak{a})$. As $v+\mathfrak{a} \in U/\mathfrak{a}$ there is some $u \in U$ such that $v+\mathfrak{a} = u+\mathfrak{a}$. But from this we find $b/u \in U^{-1}R$ and $b/u \mapsto (b+\mathfrak{a})/(u+\mathfrak{a}) = (b+\mathfrak{a})/(v+\mathfrak{a})$. Thus it remains to prove

$$\mathrm{kn}\left(\frac{b}{v} \mapsto \frac{b+\mathfrak{a}}{v+\mathfrak{a}}\right) \;=\; U^{-1}\mathfrak{a} \;=\; \left\{ \frac{a}{u} \;\middle|\; a \in \mathfrak{a}, u \in U \right\}$$

The inclusion " $\supseteq$ " is clear, given a/u where $a \in \mathfrak{a}$ we immediately find that $(a+\mathfrak{a})/(u+\mathfrak{a}) = (0 \cdot u + \mathfrak{a})/(1 \cdot u + \mathfrak{a}) = (0+\mathfrak{a})/(1+\mathfrak{a}) = 0$. Conversely consider some $b/v \in U^{-1}R$ such that $(b+\mathfrak{a})/(v+\mathfrak{a}) = 0 = (0+\mathfrak{a})/(1+\mathfrak{a})$. That is there is some $x+\mathfrak{a} \in U/\mathfrak{a}$ such that $xb+\mathfrak{a} = (x+\mathfrak{a})(b+\mathfrak{a}) = 0+\mathfrak{a}$. And this means $xb \in \mathfrak{a}$. Further - since $x+\mathfrak{a} \in U/\mathfrak{a}$ - there is some $w \in U$ such that $x+\mathfrak{a} = w+\mathfrak{a}$. That is $a := w - x \in \mathfrak{a}$. Now compute $bw = bw - bx + bx = ba + bx \in \mathfrak{a}$. Hence we found $b/v = (bw)/(vw) \in U^{-1}\mathfrak{a}$. Thus according to the isomorphism theorem $b/v \mapsto (b+\mathfrak{a})/(v+\mathfrak{a})$ induces the isomorphy as given in the claim.

(iii) We regard the homomorphism $R[t] \mapsto R_u : f \mapsto f(1/u)$. It is clear that this is surjective, since $at^k \mapsto a/u^k$ reaches all the elements of R_u. We will now show that the kernel is given to be

$$\mathrm{kn}(f \mapsto f(1/u)) \;=\; (ut-1)R[t]$$

The inclusion " $\supseteq$ " is clear, as $ut-1 \mapsto u/u - 1/1 = 0/1$. Thus suppose $f \mapsto 0/1$, then we need to show that $ut-1 \mid f$ in $R[t]$. Let $f/1 := \kappa(f) \in (U^{-1}R)[t]$ then it is clear that $1/u$ is a root

$(f/1)(1/u) = f(1/u) = 0/1$ of $f/1$ and hence $t - 1/u \mid f/1$ in $(U^{-1}R)[t]$. Since $u/1$ is a unit in R_u multiplication with $u/1$ changes nothing and hence $(ut-1)/1 \mid f/1 \in (U^{-1}R)[t]$. Thus

$$\frac{f}{1}(U^{-1}R)[t] \quad \subseteq \quad \frac{ut-1}{1}(U^{-1}R)[t]$$

But it is clear that the ideal $f/1(U^{-1}R)[t]$ corresponds to $fR[t]$ formally $(f/1(U^{-1}R)[t]) \cap R[t] = fR[t]$. And likewise the other ideal $(ut-1)/1f/1(U^{-1}R)[t]$ corresponds to $(ut-1)R[t]$. As the correspondence respects inclusions we have finally found

$$fR[t] \quad \subseteq \quad (ut-1)R[t]$$

This means $f \in (ut-1)R[t]$ and hence we have also proved "$\subseteq$". Thus $f \mapsto f(1/u)$ induces the isomorphism given its inverse is obviously given by $a/u^k \mapsto at^k + (ut-1)R[t]$.

(iv) First of all $U^{-1}R$ is an integral domain by (2.131) and hence the quotient field $\mathrm{quot}(U^{-1}R)$ is well-defined again. We will now prove the well-definedness and injectivity of the map $a/b \mapsto (a/1)/(b/1)$. As R is an integral domain (and $0 \notin U$) we get (for any a, b, c and $d \in R$)

$$\begin{aligned}
\frac{a/1}{b/1} = \frac{c/1}{d/1} \quad &\iff \quad \frac{ad}{1} = \frac{a}{1}\cdot\frac{d}{1} = \frac{b}{1}\cdot\frac{c}{1} = \frac{bc}{1} \\
&\iff \quad \exists\, u \in U \;:\; uad = ubv \\
&\iff \quad ad = bc \\
&\iff \quad \frac{a}{b} = \frac{c}{d}
\end{aligned}$$

The homomorphism property of $a/b \mapsto (a/1)/(b/1)$ is clear by definition of the addition and multiplication in localizations. Thus it only remains to check the surjectivity: consider any $(a/u)/(b/v) \in \mathrm{quot}(U^{-1}R)$, then we claim $av/bu \mapsto (a/u)/(b/v)$. To see this we have to show $(av/1)/(bu/1) = (a/u)/(b/v)$ and this follows from:

$$\frac{a}{u}\frac{bu}{1} \;=\; \frac{abu}{u} \;=\; \frac{ab}{1} \;=\; \frac{abv}{v} \;=\; \frac{b}{v}\frac{av}{1}$$

(v) We first check the well-definedness and injectivity of the map given. This can be done simultaneously by the following computation (recall that R is an integral domain and a, $b \neq 0$)

$$\begin{aligned}
\frac{x/a^h}{(b/a^n)^i} = \frac{y/a^j}{(b/a^n)^k} \quad &\iff \quad \left(\frac{b}{a^n}\right)^k \frac{x}{a^h} = \left(\frac{b}{a^n}\right)^i \frac{x}{a^j} \\
&\iff \quad \frac{xb^k}{a^{kn+h}} = \frac{yb^i}{a^{in+j}} \\
&\iff \quad xa^{in+j}b^k = ya^{kn+h}b^i \\
&\iff \quad a^{i+k}b^{h+j}\left(xa^{in+j}b^k - ya^{kn+h}b^i\right) = 0 \\
&\iff \quad xa^{in+i+j+k}b^{h+j+k} = ya^{kn+h+i+k}b^{h+i+j} \\
&\iff \quad (ab)^{j+k}xa^{(n+1)i}b^h = (ab)^{h+i}ya^{(n+1)k}b^j \\
&\iff \quad \frac{xa^{(n+1)i}b^h}{(ab)^{h+i}} = \frac{ya^{(n+1)k}b^j}{(ab)^{j+k}}
\end{aligned}$$

Hence we have a well-defined injective mapping and it is straightforward to check that it even is a homomorphism of rings. Thus it only remains to check the surjectivity. That is we are given any $x/(ab)^k \in R_{ab}$, then we obtain a preimage by

$$\frac{x/a^{(n+1)k}}{(b/a^n)^k} \;\mapsto\; \frac{xa^{(n+1)k}b^{(n+1)k}}{(ab)^{n+1)k+k}} \;=\; \frac{x}{(ab)^k}$$

(vi) Let us denote $U := R \setminus \mathfrak{p}$, as $\mathfrak{a} \subseteq \mathfrak{p}$ we get $U \cap \mathfrak{a} = \emptyset$ and $\mathfrak{a}_\mathfrak{p} = U^{-1}\mathfrak{a}$ is just the definition. Hence the claim is already included in (v).

(vii) We first show that this mapping is well defined, i.e. $u/1 \notin \overline{p}$ for $u \notin \mathfrak{p}$. But this is clear, since $\mathfrak{p} = \overline{p} \cap R$. Thus we concern ourselves with the surjectivety: given $(r/a^k)/(u/a^l) \in (R_a)_{\overline{\mathfrak{p}}}$ we see that

$$\frac{ra^l}{ua^k} \;\mapsto\; \frac{ra^l/1}{ua^k/1} \;=\; \frac{1/a^{k+l}}{1/a^{k+l}} \cdot \frac{ra^l/1}{ua^k/1} \;=\; \frac{r/a^k}{u/a^l}$$

And for the injectivety we have to consider $(r/1)/(u/1) = (s/1)/(v/1)$. Hence there is some $w/a^m \notin \overline{\mathfrak{p}}$ such that $vwr/a^m = uws/a^m \in R_a$. Thus there is some $n \in \mathbb{N}$ such that $a^{m+n}vwr = a^{m+n}uws \in R$. But $w/a^m \notin \overline{\mathfrak{p}}$ means that $w \notin \mathfrak{p}$ and as also $a \notin \mathfrak{p}$ we get that $z := a^{m+n}w \notin \mathfrak{p}$. But as $vrz = usz$ this means that $r/u = s/v \in R_\mathfrak{p}$.

□

Proof of (2.131):

- R integral domain $\implies$ $U^{-1}R$ integral domain
 Suppose $(ab)/(uv) = (a/u)(b/v) = 0/1 \in U^{-1}R$. By definition of the localization this means that there is some $w \in U$ such that $wab = 0$. But $w \neq 0$ (as $0 \notin U$) and R is an itegral domain, thus we get $ab = 0$. And this again yields $a = 0$ or $b = 0$. Of course this yields $a/u = 0/1$ or $b/v = 0/1$, that is $U^{-1}R$ is an itegral domain.

- R noetherian/artinian $\implies$ $U^{-1}R$ noetherian/artinian
 Suppose that R is noetherian and consider an ascending chain of ideals $\mathfrak{u}_1 \subseteq \mathfrak{u}_2 \subseteq \mathfrak{u}_3 \subseteq \ldots$ in $U^{-1}R$. Let us denote the corresponding ideals of R by $\mathfrak{a}_k := \mathfrak{u}_k \cap R$. Then the $\mathfrak{a}_k$ form an ascending chain $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \ldots$ of idelas of R, too. And as R is noetherian this means that there is some $s \in \mathbb{N}$ such that the chain stabilizes

 $$\mathfrak{a}_1 \;\subseteq\; \mathfrak{a}_2 \;\subseteq\; \mathfrak{a}_3 \;\subseteq\; \ldots \;\subseteq\; \mathfrak{a}_s \;=\; \mathfrak{a}_{s+1} \;=\; \mathfrak{a}_{s+2} \;=\; \ldots$$

 Yet the ideals correspond to one and another, that is $\mathfrak{u}_k = U^{-1}\mathfrak{a}_k$. So if we transfer this stabilized chain back to $U^{-1}R$ we find that

 $$\mathfrak{u}_1 \;\subseteq\; \mathfrak{u}_2 \;\subseteq\; \mathfrak{u}_3 \;\subseteq\; \ldots \;\subseteq\; \mathfrak{u}_s \;=\; \mathfrak{u}_{s+1} \;=\; \mathfrak{u}_{s+2} \;=\; \ldots$$

 the corresponding chain stabilized, too. And as the chain has been arbitrary this means, that $U^{-1}R$ is noetherian, as well. The fact that R artinian implies $U^{-1}R$ artinian can be proved in complete analogy.

- R PID $\implies$ $U^{-1}R$ PID
 Consider any ideal $\mathfrak{u} \trianglelefteq_{\mathrm{i}} U^{-1}R$, by the correspondence theorem (2.129) $\mathfrak{u}$ corresponds to the ideal $\mathfrak{a} := \mathcal{U} \cap R \trianglelefteq_{\mathrm{i}} R$ of R. But as R is a PID there is some $a \in R$ such that $\mathfrak{a} = aR$. And the following computation yields that $\mathfrak{u} = (a/1)U^{-1}R$ is a principal ideal, too

$$\mathfrak{u} \;=\; U^{-1}(aR) \;=\; \left\{ \frac{ab}{u} \;\middle|\; b \in R, u \in U \right\} \;=\; \frac{a}{1}U^{-1}R$$

- R UFD $\implies$ $U^{-1}R$ UFD
 If $0 \in U$ then $U^{-1}R = 0$ and hence $U^{-1}R$ is a UFD. Thus suppose $0 \notin U$. By definition any UFD R is an integral domain, and hence $U^{-1}R$ is an integral domain, too. Thus it suffices to check that any $a/u \in U^{-1}R$ admits a decomposition into prime factors. To see this we will first prove the following assertion

$$p \in R \text{ prime} \quad\Longrightarrow\quad \frac{p}{1} \in \left(U^{-1}R\right)^* \text{ or } \frac{p}{1} \in \left(U^{-1}R\right) \text{ prime}$$

 Thus let $p \in R$ be prime and assume $p/1 \mid (a/u)(b/v) = (ab)/(uv)$. That is there is some $h/w \in U^{-1}R$ such that $ph/w = ab/uv$. And as R is an integral domain this implies $uvph = wab$. In particular $p \mid wab$ and as p is prime this means $p \mid w$ or $p \mid a$ or $p \mid b$. First suppose $p \mid w$, i.e. there is some $\gamma \in R$ such that $\gamma p = w$. Then $(p/1)(\gamma/w) = w/w = 1$ and hence $p/1 \in (U^{-1}R)^*$ is a unit. Otherwise, if $p \mid a$ - say $\alpha p = a$ - then $(p/1)(\alpha/u) = a/u$. That is $p/1 \mid a/u$. Analogously we find $p \mid b \implies p/1 \mid b/v$. Thus either $p/1$ is a unit or prime, as claimed. Now we may easily verify that $U^{-1}R$ is an UFD: consider any $0 \neq a/u \in U^{-1}R$. As R is an UFD we find a decomposition of $a \neq 0$ into prime elements $a = \alpha p_1 \dots p_k$ (where $\alpha \in R^*$ and $p_i \in R$ prime). Now let $I := \left\{ i \in I \mid p_i/1 \in (U^{-1}R)^* \right\}$ be the set of indexes i for which $p_i/1$ is a unit. Then

$$\frac{a}{u} \;=\; \frac{\alpha}{u}\frac{p_1}{1}\cdots\frac{p_k}{1} \;=\; \left(\frac{\alpha}{u}\prod_{i\in I}\frac{p_i}{1}\right)\prod_{i\notin I}\frac{p_i}{1}$$

 That is we have found a decomposition of a/u into (a unit and) prime factors. And as a/u has been an arbitrary non-zero element, this proves that $U^{-1}R$ truly is an UFD.

- R normal $\implies$ $U^{-1}R$ normal
 We have already seen that $U^{-1}R$ is an integral domain, since R is an integral domain. To prove that $U^{-1}R$ is integrally closed in its quotient field we will make use of the isomorphy (2.132.(iii))

$$\Phi \;:\; \mathrm{QUOT}(R) \;\xrightarrow{\sim}\; \mathrm{QUOT}(U^{-1}R) \;:\; \frac{r}{s} \mapsto \frac{r/1}{s/1}$$

 Recall that R is embedded canonically into $\mathrm{QUOT}(R)$ by $a \mapsto a/1$. Hence $\mathrm{QUOT}(R)$ is considered to be an R-algebra under the scalar multiplication $a(r/s) := (a/1)\cdot(r/s) = ar/s$. Analogously, for any $a/w \in U^{-1}R$ and any r/u, $s/v \in U^{-1}R$ we have

$$\frac{a}{w}\frac{r/u}{s/v} \;=\; \frac{a/w}{1/1}\cdot\frac{r/u}{s/v} \;=\; \frac{ar/uw}{s/v}$$

 Thus if we consider any $a \in R$ and any $r/s \in \mathrm{QUOT}(R)$, then the isomorphism φ satisfies $\Phi(ax) =$

$(a/1)\Phi(x)$, which can be seen in a straightforward computation

$$\begin{aligned}\Phi(ax) &= \Phi\left(\frac{ar}{s}\right) = \frac{ar/1}{s/1} = \frac{a/1}{1/1}\cdot\frac{r/1}{s/1}\\ &= \frac{a}{1}\frac{r/1}{s/1} = \frac{a}{1}\Phi\left(\frac{r}{s}\right) = \frac{a}{1}\Phi(x)\end{aligned}$$

Now consider any $x/y \in \mathrm{quot}(U^{-1}R)$, that is integral over $U^{-1}R$. That is there are some $n \in \mathbb{N}$ and $p_0, \ldots, p_{n-1} \in U^{-1}R$ such that

$$\left(\frac{x}{y}\right)^n + \sum_{k=0}^{n-1} p_k \left(\frac{x}{y}\right)^k = 0$$

Then we need to show that $x/y \in U^{-1}R$. To do this let us pick up some $r/s \in \mathrm{quot}(R)$ such that $x/y = \Phi(r/s)$. Further note that $p_k \in U^{-1}R$, that is $p_k = a_k/u_k$ for some $a_k \in R$ and $u_k \in U$ and let $u := u_0 \ldots u_{n-1} \in U$. Then multiplication with $u^n/1 \in U^{-1}R$ yields

$$\left(\frac{u}{1}\Phi\left(\frac{r}{s}\right)\right)^n + \sum_{k=0}^{n-1} \frac{a_k u^{n-k}}{u_k}\left(\frac{u}{1}\Phi\left(\frac{r}{s}\right)\right)^k = 0$$

Now recall that $(u/1)\Phi(r/s) = \Phi(u(r/s)) = \Phi(ur/s)$. Further note that due to $k < n$ we have $u_k \mid u \mid u^{n-k}$. Therefore we may define $b_k := a_k u^{n-k}/u_k \in R$. Inserting this in the above equation yields

$$\Phi\left(\frac{ur}{s}\right)^n + \sum_{k=0}^{n-1} \frac{b_k}{1}\Phi\left(\frac{ur}{s}\right)^k = 0$$

Again we use $(b_k/1)\Phi(ur/s) = \Phi(b_k(ur/s))$ and use the homomorphism properties of Φ to place Φ in front, obtaining an equation of the form $\Phi(\ldots) = 0$. But as Φ has been an isomorphism it can be eliminated from this equation ultimatly yielding

$$\left(\frac{ur}{s}\right)^n + \sum_{k=0}^{n-1} b_k\left(\frac{ur}{s}\right)^k = 0$$

Thus we have found that $ur/s \in \mathrm{quot}(R)$ is integral over R. Hence by assumption on R we have $ur/s \in R$, that is there is some $a \in R$ such that $ur/s = a/1$. And this is $ur = as$ such that $r/s = a/u \in U^{-1}R$. Thus we have finally found

$$\frac{x}{y} = \Phi\left(\frac{r}{s}\right) = \Phi\left(\frac{a}{u}\right) = \frac{a/1}{u/1} = \frac{a/u}{1/1} \in U^{-1}R$$

- R Dedekind domain $\implies$ $U^{-1}R$ Dedekind domain
 If R is a Dedekind domain, then R is noetherian, integrally closed and $\mathrm{Spec}(R) = \{0\} \cup \mathrm{Smax}(R)$. As we have seen this implies, that $U^{-1}R$ is noetherian and integrally closed, too. Thus consider a non-zero prime ideal $0 \neq \mathfrak{w} \trianglelefteq_{\mathrm{i}} U^{-1}R$. Then $\mathfrak{m} := \mathfrak{w} \cap R \trianglelefteq_{\mathrm{i}} R$ is a non-zero prime ideal of R, too (if we had $\mathfrak{m} = 0$ then $\mathfrak{w} = U^{-1}\mathfrak{m} = 0$, a contradiction). Thus $\mathfrak{m}$ is maximal and hence $\mathfrak{w} = \mathfrak{m}R$ is maximal, too. That is $\mathrm{Spec}(U^{-1}R) = \{0\} \cup \mathrm{Smax}(U^{-1}R)$. Altogether $U^{-1}R$ is a Dedekind domain, too.

□

Proof of (3.131):

- Let us first verify (i): consider any $x/u \in U^{-1}M$, as M is generated by $\{ m_i \mid i \in I \}$ there is a finite subset $\Omega \subseteq I$ and some $a_i \in R$ such that $x = \sum_i a_i m_i$. And these can easily be used to write x/u in the following form

$$\frac{x}{u} \;=\; \sum_{i\in\Omega} \frac{a_i}{u}\frac{m_i}{1} \;\in\; \mathsf{Lh}_{U^{-1}R}\left(\left\{ \frac{m_i}{1} \;\middle|\; i \in I \right\}\right)$$

 In particular if M is a finitely generated R module, then I can be chosen to be finite itself and hence $U^{-1}M$ is a finitely generated $U^{-1}R$-module again.

- Next we will prove property (ii): that is we need to show that the subset $\{ m_i/1 \mid i \in I \}$ is linearly independent again. To do this suppose we had a finite subset $\Omega \subseteq I$ and some $a_i/u_i \in U^{-1}R$ such that

$$\frac{0}{1} \;=\; \sum_{i\in\Omega} \frac{a_i}{u}\frac{m_i}{1} \;=\; \frac{\sum_{i\in\Omega} a_i\widehat{u}_i m_i}{u}$$

 where as usual we let $u := \prod_i u_i$ (where the product runs over $i \in \Omega$) and $\widehat{u}_i := u/u_i \in U$. That is there is some $w \in U$ such that

$$0 \;=\; w\sum_{i\in\Omega} a_i\widehat{u}_i m_i \;=\; \sum_{i\in\Omega} w\widehat{u}_i a_i m_i$$

 However, as $\{ m_i \mid i \in I \}$ is R-linearly independent this implies $w\widehat{u}_i a_i = 0$ for any $i \in \Omega$. And as $w\widehat{u}_i \in U$ we obtain $a_i/u_i = 0/1$ in $U^{-1}R$ from this equality. Altogether we have proved that $\{ m_i/1 \mid i \in I \}$ truly is $U^{-1}R$-linearly independent.

- Combining (i) and (ii) we gain (iii): if $\{ m_i \mid i \in I \}$ is an R-basis of M, then $\{ m_i/1 \mid i \in I \}$ is an $U^{-1}R$ basis of $U^{-1}M$. In particular if M is free (it admits a basis) then $U^{-1}M$ is free as well (it also admits a basis). In fact this even shows the equality of the dimension

$$\dim(U^{-1}M) \;=\; \dim(M)$$

- Let us now prove that $U^{-1}M$ is noetherian again, supposed M is noetherian. I.e. we regard an ascending chain of sub-modules of $U^{-1}M$

$$Z_0 \;\subseteq\; Z_1 \;\subseteq\; \ldots \subseteq\; Z_k \;\subseteq\; Z_{k+1} \;\subseteq\; \ldots$$

 Let us denote $P_k := \overline{k}(Z_k) \;\leq_{\mathsf{m}}\; M$ then - as $\overline{k}$ respects the inclusion relation - this gives rise to an ascending chain of sub-modules of M

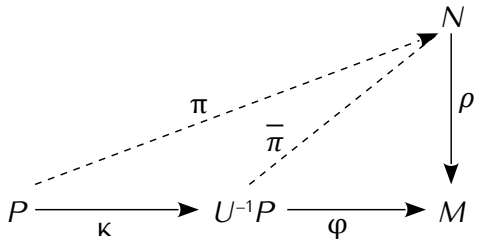
$$P_0 \;\subseteq\; P_1 \;\subseteq\; \ldots \subseteq\; P_k \;\subseteq\; P_{k+1} \;\subseteq\; \ldots$$

 Refer to (3.127) for the definition and properties of the map $\overline{k}$. But by assumption M is noetherian and hence this chain has to stabilize, that is there is some $s \in \mathbb{N}$ such that for any $i \in \mathbb{N}$ we get $P_{s+i} = P_s$. Then we get $k(P_{s+i}) = k(P_s)$ as well. But as k is the left-iverse $k\overline{k} = \mathbb{1}$ of $\overline{k}$ this

already implies $Z_{s+i} = k(P_{s+i}) = k(P_s) = Z_s$ which means that the chain of the Z_k had to stabilize. Altogether this is the noetherian property of $U^{-1}M$ again.

- From the above arguments it is clear that $U^{-1}M$ is artinian again, supposed M is artinian. All we have to do is reverse the order of inclusions, i.e. take to a descending chain instead of an ascending chain of sub-modules of $U^{-1}M$.

- Suppose P is a projective R-module, then we would like to verify that $U^{-1}P$ is a projective $U^{-1}R$-module. That is we are given another two $U^{-1}R$-modules M and N, a surjective $U^{-1}R$-module homomorphism $\varrho : N \twoheadrightarrow M$ and an arbitrary $U^{-1}R$-module homomorphism $\varphi : U^{-1}P \to M$. The projective property demands the existence (but not the uniqueness) of another $U^{-1}R$-module homomorphism $\overline{\pi} : U^{-1}P \to N$, such that $\varphi = \varrho\overline{\pi}$. But as P is projective by assumption we may expand this diagram, and use the projective property of P:



That is we pick up the R-module homomorphism $\pi : P \to N$ such that $\varphi\kappa = \varrho\pi$. Then we take $\overline{\pi} : U^{-1}P \to N : x/u \mapsto (1/u)\pi(x)$, that is $\overline{\pi}$ is $U^{-1}\pi$ appended, by $y/u \mapsto (1/u)y$. Hence it is clear that $\overline{\pi}$ is a well-defined $U^{-1}R$-module homomorphism again, due to (3.125.(ii)). We now need to verify $\varphi = \varrho\overline{\pi}$. But this can be done in a simple computation, using the $U^{-1}R$-linearity of ϱ and φ

$$\varrho\overline{\pi}\left(\frac{1}{u}\pi(x)\right) \;=\; \frac{1}{u}\varrho\pi(x) \;=\; \frac{1}{u}\varphi\kappa(x) \;=\; \frac{1}{u}\varphi\left(\frac{x}{1}\right) \;=\; \varphi\left(\frac{x}{1}\right)$$

- Suppose I is an injective R-module, then we would like to verify that $U^{-1}I$ is an injective $U^{-1}R$-module. One of the equivalent properties of being injective is the following: given a sub-module $Q \leq_{\mathfrak{m}} I$ of I there already in another sub-module $P \leq_{\mathfrak{m}} I$ such that $I = P + Q$ and $P \cap Q = 0$ (that is Q is a direct summand of I). Thus consider any $U^{-1}R$-sub-module $Q \leq_{\mathfrak{m}} U^{-1}I$. According to (3.127) Z corresponds to a sub-module $Q \leq_{\mathfrak{m}} I$ of I by virtue of $Z = U^{-1}Q$. And due to the injectivity this gives rise to $P \leq_{\mathfrak{m}} I$ as described above. Now let $Y := U^{-1}P \leq_{\mathfrak{m}} U^{-1}I$ then it is clear, that $Y + Z \subseteq U^{-1}I$. Conversely consider any $x/u \in U^{-1}I$, that is $u \in U$ and $x \in I$. As $I = P + Q$ there are some $p \in P$ and $q \in Q$ such that $x = p + q$. But from this we get $x/u = (p+q)/u = p/u + q/u \in Y + Z$. It remains to verify $Y \cap Z = 0$ but this follows from (3.127) again

$$Y \cap Z \;=\; U^{-1}P \cap U^{-1}Q \;=\; U^{-1}\Big(P \cap Q\Big) \;=\; U^{-1}0 \;=\; 0$$

□

Proof of (3.135):
Clearly (a) $\Longrightarrow$ (b) and (b) $\Longrightarrow$ (c) are trivial. Hence we only need to consider (c) $\Longrightarrow$ (a). Thus suppose we had (c) but $M \neq 0$. That is we could choose some $x \in M$ with $x \neq 0$. Then we take to

the annihilator $\mathfrak{a} := \mathrm{ann}(x) := \{\, a \in R \mid ax = 0 \,\}$ of x. As $x \neq 0$ we have $\mathfrak{a} \neq R$ and hence (2.4.(ii)) tells us that $\mathfrak{a}$ is contained $\mathfrak{a} \subseteq \mathfrak{m}$ inside a maximal ideal $\mathfrak{m} \trianglelefteq_{\mathrm{i}} R$. By assumption we have $M_{\mathfrak{m}} = 0$ in particular $x/1 = 0/1$ in $M_{\mathfrak{m}}$. This means there is some $w \in U = R \setminus \mathfrak{m}$ such that $wx = 0$. But by definition of $\mathfrak{a}$ this is $w \in \mathfrak{a} \subseteq \mathfrak{m}$. This of course is a contradiction and hence we have $M = 0$. □

Proof of (3.136):
In a first step we will prove that $x = 0$ is equivalent to $x/1 = 0/1$ in $M_{\mathfrak{m}}$ for any maximal ideal $\mathfrak{m} \trianglelefteq_{\mathrm{i}} R$. Let us denote $L := Rx$ the sub-module of M generated by x. Then $x = 0$ is equivalent to $L = 0$. And due to (3.135) this again is equivalent to $L_{\mathfrak{m}} = 0$ for any $\mathfrak{m} \in \mathrm{Smax}(R)$. As L is generated by x we know that $L_{\mathfrak{m}}$ is generated by $x/1$ - that is $L_{\mathfrak{m}} = R_{\mathfrak{m}}(x/1)$ according to (3.131.(ii)). Hence $L_{\mathfrak{m}} = 0$ is equivalent to $x/1 = 0/1$ and altogether we have

$$x = 0 \iff \forall\, \mathfrak{m} \in \mathrm{Smax}(R) \,:\, \frac{x}{1} = \frac{0}{1}$$

Now consider the sub-module $P \leq_{\mathfrak{m}} M$. Then $x \in P$ is equivalent to $x + P = 0 + P$ in the quotient module M/P. And by the above this is equivalent to $(x + P)/1 = (0 + P)/1$ in $(M/P)_{\mathfrak{m}}$ (for any $\mathfrak{m} \in \mathrm{Smax}(R)$). We now use the isomorphy of the quotients as proved in (3.125.(i)). That is $(M/P)_{\mathfrak{m}} \xrightarrow{\sim} M_{\mathfrak{m}}/P_{\mathfrak{m}}$ under the isomorphism $(x + P)/u \mapsto x/u + P_{\mathfrak{m}}$. Applying this isomorphism we have found another equivalent reformulation: for any $\mathfrak{m} \in \mathrm{Smax}(R)$ we have $x/1 + P_{\mathfrak{m}} = 0/1 + P_{\mathfrak{m}}$ in $M_{\mathfrak{m}}/P_{\mathfrak{m}}$. And this again is $x/1 \in P_{\mathfrak{m}}$ for any $\mathfrak{m} \in \mathrm{Smax}(R)$, as has been claimed. □

Proof of (3.137):
The implications (a) $\implies$ (b) are either trivial or have been shown in (3.125.(ii)). Also the implication (b) $\implies$ (c), as every maximal ideal of R already is prime. It remains to verify (c) $\implies$ (a) in the respective cases: *Injective:* let $P := \mathrm{kn}(\varphi)$, then for any maximal ideal $\mathfrak{m} \trianglelefteq_{\mathrm{i}} R$ we have $P_{\mathfrak{m}} = \mathrm{kn}(\varphi_{\mathfrak{m}})$ according to (3.127.(ii)). And as any $\varphi_{\mathfrak{m}}$ is injective this makes $P_{\mathfrak{m}} = 0$. Now suppose we have some $x \in P$ then by (3.136) this is equivalent to $x/1 \in P_{\mathfrak{m}} = 0$ for any maximal ideal $\mathfrak{m}$, such that always $x/1 = 0/1$. But this again means $x = 0$, so we have proved $x \in \mathrm{kn}(\varphi) \implies x = 0$ which is the injectivity of φ.

Surjective: let $Q := \mathrm{im}(\varphi)$, then for any maximal ideal $\mathfrak{m} \trianglelefteq_{\mathrm{i}} R$ we have $Q_{\mathfrak{m}} = \mathrm{im}(\varphi_{\mathfrak{m}})$ according to (3.127.(ii)). And as any $\varphi_{\mathfrak{m}}$ is surjective this makes $Q_{\mathfrak{m}} = N_{\mathfrak{m}}$. Now pick up any $y \in N$, then $x/1 \in N_{\mathfrak{m}} = Q_{\mathfrak{m}}$ for any $\mathfrak{m} \in \mathrm{Smax}(R)$. And by (3.136) this implies $y \in Q = \mathrm{im}(\varphi)$. As y has been arbitrary this is the surjectivity of φ.

Bijective: if all the $\varphi_{\mathfrak{m}}$ are bijective, they are both injective and surjective. Hence by the above φ itself is injective and surjective, hence bijective, again. *Zero:* let $Q := \mathrm{im}(\varphi)$ again, then (as any $\varphi_{\mathfrak{m}} = 0$) this time we get $Q_{\mathfrak{m}} = 0$ for any maximal ideal $\mathfrak{m} \in R$. By (3.136) once more, this yields $Q = 0$ and hence $\varphi = 0$, as well. □

Proof of (3.133):
We first need to check that h is well-defined, that is consider any two homomorphisms $\varphi, \psi : M \to N$ and $u, v \in U$ such that $\varphi/u = \psi/v$. That is there is some $w \in U$ such that $wv\varphi = wu\varphi$. If we are now given any $x/q \in U^{-1}M$, then multiplying this equation with q and inserting x we get $wqv\varphi(x) = wqu\psi(x)$. And this again is $h(\varphi/u)(x/q) = \varphi(x)/qu = \psi(x)/qv = h(\psi/v)(x/q)$. And as x/q has been arbitrary this is $h(\varphi/u) = h(\psi/v)$. The next step is verifying the properties of an R-module homomorphism: that

is we consider φ/u and ψ/v again. Then $\varphi/u + \psi/v = (v\varphi + u\psi)/uv$, which is mapped to

$$h\left(\frac{\varphi}{u}+\frac{\psi}{v}\right)\left(\frac{x}{q}\right) \;=\; \frac{v\varphi(x)+u\psi(x)}{quv} \;=\; \frac{\varphi(x)}{qu}+\frac{\psi(x)}{qv}$$

That is the image of the sum of the homomorphisms $h(\varphi/u + \psi/v)$ is the sum of the images $h(\varphi/u) + h(\psi/v)$. Also it is straightforward to prove the $U^{-1}R$-linearity of h: as $(a/u)(\psi/v) = a\psi/uv$ we get

$$h\left(\frac{a}{u}\frac{\psi}{v}\right)\left(\frac{x}{q}\right) \;=\; \frac{a\psi(x)}{quv} \;=\; \frac{a}{u}\frac{\psi(x)}{qu}$$

To prove item (i) we assume that $M = \mathrm{Lh}_R\{\, m_1, \ldots, m_n \,\}$ for some $m_i \in M$. Now suppose we had $h(\varphi/u) = 0$ for some $\varphi : M \to N$ and $u \in U$. I.e. for any $x/q \in U^{-1}M$ we have $\varphi(x)/qu = 0/1$ and hence there is some $w \in U$ such that $w\varphi(x) = 0$. In particular we may choose some $w_i \in U$ such that $w_i\varphi(m_i) = 0$. Now let $w := w_1 \ldots w_n$ and $\widehat{w}_i := w/w_i \in U$. As the m_i generate M any $x \in M$ can be written as $x = a_1m_1 + \cdots + a_nm_n$ for some $a_i \in R$ such that the R-linearity of φ yields

$$w\varphi(x) \;=\; w\sum_{i=1}^{n} a_i\varphi(m_i) \;=\; \sum_{i=1}^{n} a_i\widehat{w}_i w_i\varphi(m_i) \;=\; 0$$

That is $w\varphi(x) = 0$ and as $x \in M$ has been arbitrary, this is $w\varphi = 0$. This again means $\varphi/u = 0/1$ is the zero-homomorphism, shuch that the kernel of h is 0, which is the injectivity of h.

Let us now prove item (ii): If M admits a finite free presentation, then it is finitely generated already (see below). In particular we already know, that h is injective and it remains to prove the surjectivity of h. Recall that the finite free presentation is an exact chain of the form

$$R^m \;\xrightarrow{\;\alpha\;}\; R^n \;\xrightarrow{\;\omega\;}\; M \to 0$$

Reasoning: let e_i (where $i \in 1 \ldots m$) be the Euclidean basis of R^m. As ω is surjective the $m_i := \omega(e_i)$ (where $i \in 1 \ldots m$) build up a generating set of M and hence $\mathrm{rank}(M) \leq m$ is finitely generated. In particular, according to (3.131.(i)), $U^{-1}M$ is generated by the $m_i/1$ (where $i \in 1 \ldots m$). Let us now pick up the Euclidean basis $f_j \in R^n$ (where $j \in 1 \ldots n$) of R^n as well and denote $A_j := \alpha(f_j) \in R^m$. That is $A_j = (A_{1,j}, \ldots, A_{m,j})$ for some $A_{i,j} \in R$. That is, if $a = (a_1, \ldots, a_n) \in R^n$ then we have

$$\alpha(a) \;=\; \sum_{j=1}^{n} a_j\alpha(f_j) \;=\; \sum_{j=1}^{n} a_j \sum_{i=1}^{m} A_{i,j}e_i \;=\; \sum_{i=1}^{m}\left(\sum_{j=1}^{n} A_{i,j}a_j\right)e_i$$

As $\mathrm{im}(\alpha) = \mathrm{kn}(\omega)$ we have (for any $b \in R^m$) the equivalence $\omega(b) = 0$ if and only if $b = \alpha(a)$ for some $a \in R^n$. Writing $b = (b_1, \ldots, b_m) \in R^m$ again we see $\omega(b) = \sum_i b_i\omega(e_i) = \sum_i b_im_i$ such that this equivalence turns into

$$\sum_{i=1}^{m} b_im_i = 0 \quad\Longleftrightarrow\quad \exists\, a \in R^n \;\; \forall\, j \in 1 \ldots n \;\;:\;\; b_i = \sum_{j=1}^{n} A_{i,j}a_j$$

In particular $\omega(A_j) = \sum_i A_{i,j}m_i = 0$ since $A_j = \alpha(f_j)$ for any $j \in 1 \ldots n$. Then, in the localization $U^{-1}M$

of M, we get the equality

$$\frac{0}{1} \;=\; \frac{\sum_{i=1}^m A_{i,j} m_i}{1} \;=\; \sum_{i=1}^m \frac{A_{i,j}}{1}\frac{m_i}{1}$$

After all these preparations suppose we are given some $U^{-1}R$-module homomorphism $\psi : U^{-1}M \to U^{-1}N$. Let us denote $n_i/u_i := \psi(m_i/1)$ for some $n_i \in N$ and $u_i \in U$. Let us also denote $u := u_1 \cdot \dots \cdot u_m$ and $\widehat{u}_i := u/u_i \in U$ as usual. Note that ψ is determined by its action on the $m_i/1$, as these elements generate $U^{-1}M$. Then due to the linearity of ψ the above equation turns into the following equation of $U^{-1}N$

$$\frac{0}{1} \;=\; \psi\left(\sum_{i=1}^m \frac{A_{i,j}}{1}\frac{m_i}{1}\right) \;=\; \sum_{i=1}^m \frac{A_{i,j}}{1}\frac{n_i}{u_i} \;=\; \frac{\sum_{i=1}^m A_{i,j}\widehat{u}_i n_i}{u}$$

By definition of the localization that is (for any $j \in 1 \dots n$) there is some $w_j \in U$ such that $w_j \sum_i A_{i,j}\widehat{u}_i n_i = 0$. Again we denote $w := w_1 \cdot \dots \cdot w_n$ and $\widehat{w}_j := w/w_j \in U$. This enables us to define or candidate for the R-module homomorphism $\varphi : M \to N$ by linear expansion of $\varphi(m_i) := w\widehat{u}_i n_i$. If this is well-defined then it automatically yields an R-linear map. To prove the well-definedness we have to regard $\sum_i a_i m_i = \sum_i a'_i m_i$ and need to show that this implies $\sum_i a_i w\widehat{u}_i n_i = \sum_i a'_i w\widehat{u}_i n_i$. By going to differences $b_i = a'_i - a_i$ it hence suffices to check

$$\sum_{i=1}^m b_i m_i \;=\; 0 \quad\Longrightarrow\quad \sum_{i=1}^m b_i w\widehat{u}_i n_i \;=\; 0$$

But due to $\mathrm{im}(\alpha) = \mathrm{kn}(\omega)$ we have seen above that $\sum_i b_i m_i = 0$ is equivalent to $b_i = \sum_j A_{i,j} a_j$ for some $a_j \in R$ and any $i \in 1 \dots m$. Hence the latter sum turns into

$$\sum_{i=1}^m b_i w\widehat{u}_i n_i \;=\; \sum_{i=1}^m \sum_{j=1}^n A_{i,j} a_j w\widehat{u}_i n_i \;=\; \sum_{j=1}^n a_j \widehat{w}_j w_j \sum_{i=1}^m A_{i,j}\widehat{u}_i n_i \;=\; 0$$

by choice of the w_j (see above). That is φ is truly well-defined. And all we have left to do is check that $h(\varphi/uw) = \psi$. But as the $m_i/1$ generate $U^{-1}M$ it suffices to prove this for all the $m_i/1$. And this can be done in a last simple computation

$$\frac{U^{-1}\varphi(m_i/1)}{uw} \;=\; \frac{\varphi(m_i)}{uw} \;=\; \frac{w\widehat{u}_i n_i}{uw} \;=\; \frac{n_i}{u_i} \;=\; \varphi\left(\frac{m_i}{1}\right)$$

□

Proof of (2.134):

We have already proved (a) $\Longrightarrow$ (b) in (2.131) and (b) $\Longrightarrow$ (c) is trivial. Thus it only remains to verify (c) $\Longrightarrow$ (a): we denote $F := \mathrm{QUOT}(R)$ the quotient field of R and regard R and any localization $R_{\mathfrak{m}}$ as a sub-ring of R (also refer to (2.133) for this). Now regard any $x \in F$ integral over R, that is $f(x) = 0$ for some normed polynomial $f \in R[t]$. If we interpret $f \in R_{\mathfrak{m}}[t]$, then $f(x) = 0$ again and hence x is integral over $R_{\mathfrak{m}}$ (where $\mathfrak{m} \trianglelefteq_{\mathrm{i}} R$ is any maximal ideal of R). By assumption $R_{\mathfrak{m}}$ is normal and hence $x \in R_{\mathfrak{m}}$ again. And as $\mathfrak{m}$ has been arbitrary the local global principle (2.133) yields:

$$x \;\in\; \bigcap_{\mathfrak{m}\in \mathrm{smax}R} R_{\mathfrak{m}} \;=\; R$$

□

Proof of (2.60): (continued)

- (c) $\implies$ (d): property (2) of (c) and (d) are identical so we only need to verify (1) in (d). If all $a_i = 0$ are zero then there is nothing to prove ($s := 0$). And if at least one $a_r \neq 0$ is non-zero, then so are all a_{r+i} for $i \in \mathbb{N}$. Omitting the a_0 to a_{r-1} we may assume $a_i \neq 0$ for any $i \in \mathbb{N}$. By assumption we have $a_i R \subseteq a_{i+1} R$ for any $i \in \mathbb{N}$. And this translates into $a_{i+1} \mid a_i$. By (2.64.(iii)) this yields a descending chain of natural numbers for any prime element $p \in R$

$$\langle p \mid a_0 \rangle \ \geq \ \langle p \mid a_1 \rangle \ \geq \ \ldots \ \geq \ \langle p \mid a_i \rangle \ \geq \ \ldots \geq 0$$

 Of course this means that the sequence $\langle p \mid a_i \rangle$ has to become startionary. That is there is some $s(p) \in \mathbb{N}$ such that for all $i \in \mathbb{N}$ we get $\langle p \mid a_{s(p)+i} \rangle = \langle p \mid a_{s(p)} \rangle$. We now choose a representing system $\mathbb{P}$ of the prime elements of R modulo associateness. Then there only are *finitely many* $p \in \mathbb{P}$ such that $\langle p \mid a_0 \rangle \neq 0$. And for those $p \in \mathbb{P}$ with $\langle p \mid a_0 \rangle = 0$ we may clearly take $s(p) = 0$. Thereby we may define

$$s \ := \ \max\{\, s(p) \mid p \in \mathbb{P} \,\} \ \in \ \mathbb{N}$$

 Then it is clear that for any $p \in \mathbb{P}$ and any $i \in \mathbb{N}$ we get $\langle p \mid a_{s+i} \rangle = \langle p \mid a_s \rangle$. And by (2.64.(iv)) this is nothing but $a_{s+i} \approx a_s$ which again translates into $a_{s+i} R = a_s R$. And this is just what had to be proved.

- (d) $\implies$ (c): property (2) of (c) and (d) are identical so we only need to verify (1) in (c). But the proof of this would be a literal repetition of (2.59.(iii)). There we have proved the existence of an irreducible decomposition using the ascending chain condition of noetherian rings. But in fact this property has only been used for principal ideals and hence is covered by the assumption (1) in (d). Hence the same proof can be applied here, too.

- (a) $\implies$ (e): As $\mathfrak{p} \neq 0$ is non-zero, there is some $0 \neq a \in R$ with $a \in \mathfrak{p}$. Clearly $a \notin R^*$ as else $\mathfrak{p} = R$. We now use a prime decomposition of a, that is $\alpha p_1 \ldots p_k = a \in \mathfrak{p}$. Thereby $k \geq 1$ as else $a \in R^*$. And as $\mathfrak{p}$ is prime we either get $\alpha \in \mathfrak{p}$ or $p_i \in \mathfrak{p}$ for some $i \in 1 \ldots k$. But again $\alpha \in \mathfrak{p}$ would yield $\mathfrak{p} = R$ which cannot be. Thus $p := p_i \in \mathfrak{p}$ where p is prime by construction.

- (e) $\implies$ (f): We assume $R \neq 0$ (else the stetements herin do not make sense!). It is clear that $0 \notin D$ (as R is an integral domain $\alpha \in R^*$ and $p_i \neq 0$). Therefore $D \subseteq R \setminus \{0\}$ such that we obtain the canonical homomorphism

$$D^{-1}R \to \mathrm{quot}(R) \ : \ \frac{a}{d} \mapsto \frac{a}{d}$$

 Due to $0 \notin D$ we also see that $D^{-1}R \neq 0$ is not the zero-ring. Therefore $D^{-1}R$ contains a maximal ideal $\mathfrak{u} \trianglelefteq_{\mathrm{i}} D^{-1}R$ - by (2.4.(iv)) - such that $\mathfrak{p} := \mathfrak{u} \cap R \in D^{-1}\mathrm{Smax}(R)$ is maximal too - by (2.129) - in particular prime. Suppose $\mathfrak{p} \neq 0$ then by assumption (e) there is some prime element $p \in \mathfrak{p}$. And thereby $p \in \mathfrak{p} \cap D$ in contradiction to $\mathfrak{p} \in D^{-1}\mathrm{Smax}(R)$. Thus $\mathfrak{p} = 0$ and therefore $\mathfrak{u} = D^{-1}\mathfrak{p} = 0$, too. But $0 \in D^{-1}R$ being maximal yields that $D^{-1}R$ is a field. In particular the canonical homomorphism is injective (as it is non-zero). Now choose any $a/b \in \mathrm{quot}(R)$ then a, $b \in R$ and hence $a/1$, $b/1 \in D^{-1}R$. Yet $b \neq 0$ and hence $(1/b)^{-1} = 1/b \in D^{-1}R$, as $D^{-1}R$ is a field. Therefore $a/b \in D^{-1}R$ such that the canonical homomorphism also is surjective. By

construction this even is an equality of sets.

- (f) $\implies$ (a): Consider any $0 \neq a \in R$. Then $1/a \in \text{QUOT}(R) = D^{-1}R$, that is there are $b \in R$ and $d \in D$ such that $1/a = b/d$. And as R is an integral domain this is $ab = d \in D$. Yet D is saturated by (2.58.(vi)) and therefore $a \in D$. But this just means that a admits a prime decomposition.

□

Proof of (2.90):
We have already proved statements (i) to (vii) on page (1059), so it only remains to prove statement (viii). We have already seen in (vii) that the map $\mathfrak{b} \mapsto \mathfrak{b} \cap R = \kappa^{-1}(\mathfrak{b})$ is well-defined (as $\kappa^{-1}(\mathfrak{q}) = \mathfrak{q} \cap R = \mathfrak{p}$ again). Thus we next check the well-definedness of $\mathfrak{a} \mapsto U^{-1}\mathfrak{a}$. First of all we have $\sqrt{U^{-1}\mathfrak{a}} = U^{-1}\sqrt{\mathfrak{a}} = U^{-1}\mathfrak{p} = \mathfrak{q}$ due to (2.125). Now consider a/u and $b/v \in U^{-1}R$ such that $(ab)/(uv) = (a/u)(b/v) \in U^{-1}\mathfrak{a}$ but $b/v \notin U^{-1}R$. Then $ab \in (U^{-1}\mathfrak{a}) \cap R = \mathfrak{a} : U$, that is there is some $w \in U$ such that $abw \in \mathfrak{a}$. But $bw \notin \mathfrak{a}$, as else $b/v = (bw)/(vw) \in U^{-1}\mathfrak{a}$. As $\mathfrak{a}$ is primary this implies $a \in \sqrt{\mathfrak{a}} = \mathfrak{p}$ and hence $a/u \in U^{-1}\mathfrak{p} = \mathfrak{q} = \sqrt{U^{-1}\mathfrak{a}}$. This means that $U^{-1}\mathfrak{a}$ is primary again and hence $\mathfrak{a} \mapsto U^{-1}\mathfrak{a}$ is well-defined. □

Proof of (2.19):

(i) As the union ranges over all prime ideals $\mathfrak{p}$ with $\mathfrak{p} \subseteq \text{ZD}(R)$ it is clear that the union is contained in $\text{ZD}(R)$ again. That is the incluison " $\supseteq$ " is trivial. For the converse inclusion let us denote $U := \text{NZD}R$, then U is multiplicatively closed. Let now $a \in \text{ZD}(R)$ be a zero-divisor. That is we may choose some $0 \neq b \in R$ such that $ab = 0$. This implies $aR \subseteq \text{ZD}(R)$ (because given any $x \in R$ we get $(ax)b = x(ab) = x0 = 0$) or in other words $aR \cap U = \emptyset$. Thus by (2.4.(iii)) we may choose an ideal $\mathfrak{p}$ maximal among the ideals satisfying $aR \subseteq \mathfrak{b} \subseteq R \setminus U = \text{ZD}(R)$ and this is prime. In particular $a \in \mathfrak{p}$ such that a is also contained in the union of prime ideals contained in $\text{ZD}(R)$.

(ii) Let $\mathfrak{p}$ be a minimal prime ideal of R, then by the correspondence theorem (2.129) the spectrum of the localized ring $R_\mathfrak{p}$ corresponds to

$$\text{Spec}(R_\mathfrak{p}) \longleftrightarrow \{\, \mathfrak{q} \in \text{Spec}(R) \mid \mathfrak{q} \subseteq \mathfrak{p} \,\} \longleftrightarrow \{\, \mathfrak{p} \,\}$$

Hence $R_\mathfrak{p}$ has precisely one prime ideal, namely the ideal $\overline{\mathfrak{p}} = (R \setminus \mathfrak{p})^{-1}\mathfrak{p}$ corresponding to $\mathfrak{p}$. And by (2.22.(v)) this yields

$$\text{NIL}(R_\mathfrak{p}) = \bigcap \text{Spec}(R_\mathfrak{p}) = \overline{\mathfrak{p}}$$

Now consider any $a \in \mathfrak{p}$, then $a/1 \in \overline{\mathfrak{p}}$ and hence there is some $k \in \mathbb{N}$ such that $a^k/1 = (a/1)^k = 0/1$. That is there is some $u \in R \setminus \mathfrak{p}$ such that $ua^k = 0$. But $k \neq 0$ as else $u = 0 \in \mathfrak{p}$. Hence we may choose $1 \leq k$ minimally such that $ua^k = 0$. Then we let $b := ua^{k-1}$ and thereby get $b \neq 0$ (as k has been minimal) and $ab = 0$. That is $a \in \text{ZD}(R)$ and hence $\mathfrak{p} \subseteq \text{ZD}R$ (as a has been arbitrary).

(iii) As R is commutative, we know from (1.47.(vi)) that $\text{NIL}(R)$ is an ideal. If $R = 0$, then $R/\text{NIL}(R) = 0$ is the zero-ring, too. Hence neither of these rings has any prime ideal and hence $\emptyset \longleftrightarrow \emptyset$ is trivial. So let now $R \neq 0$ and consider any prime ideal $\mathfrak{p} \trianglelefteq_\text{i} R$ and any $a \in R$ with $a^n = 0 \in \mathfrak{p}$. If $n = 0$ then $1 = 0$, which we excluded by $R \neq 0$. As $\mathfrak{p}$ is a prime ideal, we conclude $a \in \mathfrak{p}$. And as $\mathfrak{p}$ and a have been arbitrary, this means $\text{NIL}(R) \subseteq \mathfrak{p}$. Then the claim is just a special case of the

correspondence theorem of ideals (1.71) in quotient rings:

$$\operatorname{Spec}\left(R \big/ \operatorname{NIL}(R)\right) \;\longleftrightarrow\; \{\, \mathfrak{p} \in \operatorname{Spec}(R) \mid \operatorname{NIL}(R) \subseteq \mathfrak{p} \,\} \;=\; \operatorname{Spec}(R)$$

□

Proof of (2.135):
(b) $\Longrightarrow$ (a): of course $R = 0$ cannot occur, as else $R^* = R$ and hence $R \setminus R^* = \emptyset$ was no ideal of R. Thus $R \neq 0$ and hence R contains a maximal ideal, by (2.4.(iv)). And if $\mathfrak{m} \trianglelefteq_{\mathrm{i}} R$ is any maximal ideal of R then we have $\mathfrak{m} \neq R$ and hence $\mathfrak{m} \subseteq R \setminus R^* \neq R$. By maximality of $\mathfrak{m}$ we get $\mathfrak{m} = R \setminus R^*$ which also is the uniqueness of the maximal ideal. (a) $\Longrightarrow$ (b): let $\mathfrak{m}$ be the one and only maximal ideal of R. As $\mathfrak{m} \neq R$ we again get $\mathfrak{m} \subseteq R \setminus R^*$. Conversely, if $a \in R \setminus R^*$ then $aR \neq R$. Hence there is a maximal ideal containing aR, by (2.4.(ii)). But the only maximal ideal is $\mathfrak{m}$ such that $a \in aR \subseteq \mathfrak{m}$. And as a has been arbitrary this proves $R \setminus R^* \subseteq \mathfrak{m}$ and hence $\mathfrak{m} = R \setminus R^*$. In particular $R \setminus R^*$ is an ideal of R. □

Proof of (2.136):
(a) $\Longrightarrow$ (b): consider any $\mathfrak{a} \neq R$, then by (2.4.(ii)) $\mathfrak{a}$ is contained in some maximal ideal, and the only maximal ideal available is $\mathfrak{m}$, such that $\mathfrak{a} \subseteq \mathfrak{m}$. (b) $\Longrightarrow$ (a): first of all $\mathfrak{m}$ is a maximal ideal, as (due to (b)) $\mathfrak{m} \subseteq \mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ implies $\mathfrak{m} = \mathfrak{a}$ or $\mathfrak{a} = R$. And if $\mathfrak{n} \trianglelefteq_{\mathrm{i}} R$ is any maximal ideal of R, then we have $\mathfrak{n} \neq R$ and hence (due to (b)) $\mathfrak{n} \subseteq \mathfrak{m}$. But by maximality of $\mathfrak{n}$ and $\mathfrak{m} \neq R$ we now conclude $\mathfrak{n} = \mathfrak{m}$. Altogether we have $\operatorname{Smax}(R) = \{\mathfrak{m}\}$ as claimed. (a) $\Longrightarrow$ (c): has already been proved in (2.135) - in the form $R \setminus R^* = \mathfrak{m}$. (c) $\Longrightarrow$ (d) is trivial, so it only remains to prove the implication (d) $\Longrightarrow$ (b): consider any ideal $\mathfrak{a} \neq R$ again, then we have $\mathfrak{a} \subseteq R \setminus R^*$ and due to (d) this yields $\mathfrak{a} \subseteq R \setminus R^* \subseteq \mathfrak{m}$. □

Proof of (2.138):
First of all any $R \setminus \mathfrak{q}_i$ is multiplicatively closed, as $\mathfrak{q}_i$ is a prime ideal. The intersection of multiplicatively closed sets is multiplicatively closed again, so $U = R \setminus Q$ is multiplicatively closed.By the correspondence theorem (2.129) we know that the prime spectrum of $U^{-1}R$ is given to be

$$\operatorname{Spec}(U^{-1}R) \;=\; \left\{\, U^{-1}\mathfrak{p} \mid \mathfrak{p} \in \operatorname{Spec}(R), \mathfrak{p} \cap U = \emptyset \,\right\}$$

But $\mathfrak{p} \cap (R \setminus Q) = \emptyset$ is equivalent to $\mathfrak{p} \subseteq Q$, where $Q = \mathfrak{q}_1 \cup \cdots \cup \mathfrak{q}_n$. Now by prime avoidance (2.14.(iii)) there is some $i \in 1 \ldots n$ such that $\mathfrak{p} \subseteq \mathfrak{q}_i$. If $\mathfrak{q}_i$ is not maximal in $\mathcal{Q}$ itself, then there is a maximal $\mathfrak{q}_j \in \mathcal{Q}$ containing $\mathfrak{q}_i \subseteq \mathfrak{q}_j$. And of course if $\mathfrak{p} \subseteq \mathfrak{q}$ for some $\mathfrak{q} \in \mathcal{Q}^*$ then $\mathfrak{p} \subseteq Q$ is a given. Hence we can reformulate $\operatorname{Spec}(U^{-1}R)$ as claimed:

$$\operatorname{Spec}(U^{-1}R) \;=\; \left\{ U^{-1}\mathfrak{p} \;\middle|\; \begin{array}{l} \mathfrak{p} \in \operatorname{Spec}(R) \text{ such that} \\ \exists\, \mathfrak{q} \in \mathcal{Q}^* \ldots n : \mathfrak{p} \subseteq \mathfrak{q} \end{array} \right\}$$

Next we prove the equality for the maximal ideals: By the correspondence theorem (2.129) we also know that the maximal ideals of $U^{-1}R$ correspond to the ideals $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ that are maximal with respect to the property $\mathfrak{a} \subseteq Q$. That is

$$\operatorname{Smax}(U^{-1}R) \;=\; \left\{ U^{-1}\mathfrak{m} \;\middle|\; \begin{array}{l} \mathfrak{m} \trianglelefteq_{\mathrm{i}} R \text{ with } \mathfrak{m} \subseteq Q \text{ and} \\ \mathfrak{m} \subseteq \mathfrak{a} \subseteq Q \implies \mathfrak{m} = \mathfrak{a} \end{array} \right\}$$

In particular any ideal $\mathfrak{q} \in \mathcal{Q}^*$ qualifies for this property, as $\mathfrak{q} \subseteq \mathfrak{a} \subseteq Q$ implies $\mathfrak{q} \subseteq \mathfrak{a} \subseteq \mathfrak{q}_i$ for some

$i \in 1 \ldots n$ and hence $\mathfrak{q} = \mathfrak{q}_i$ such that $\mathfrak{q} = \mathfrak{a}$. Conversely, if $\mathfrak{m} \subseteq Q$ is any ideal, then we already have $\mathfrak{m} \subseteq \mathfrak{q}_i$ for some $i \in 1 \ldots n$ by prime avoidance, again. Pick up a maximal ideal $\mathfrak{q}_j \in \mathcal{Q}^*$ containing $\mathfrak{q}_i \subseteq \mathfrak{q}_j$. Then we have $\mathfrak{m} \subseteq \mathfrak{q}_j \subseteq Q$ such that by assumption of $\mathfrak{m}$ we get $\mathfrak{m} = \mathfrak{q}_j \in \mathcal{Q}^*$. Therefore the $U^{-1}\mathfrak{q}_j$ with $\mathfrak{q}_j \in \mathcal{Q}^*$ are the only maximal ideals of $U^{-1}R$.

$$\operatorname{Smax}(U^{-1}R) \;=\; \left\{ U^{-1}\mathfrak{m} \mid \mathfrak{m} \in \mathcal{Q}^* \right\}$$

If $\mathcal{Q} = \{ \mathfrak{p} \}$ contains one element only, then $\mathcal{Q}^* = \{ \mathfrak{p} \}$, as there is no other ideal in $\mathcal{Q}$ that could be larger. In particular $U^{-1}\mathfrak{p} = \mathfrak{m}_\mathfrak{p}$ is the one and only maximal ideal of $U^{-1}R = R_\mathfrak{p}$ as we have just argued above. That is $R_\mathfrak{p}$ is a local ring.with maximal ideal $\mathfrak{m}_\mathfrak{p}$.
Now regard $R_\mathfrak{p} \twoheadrightarrow \operatorname{QUOT}(R)/\mathfrak{p} : a/u \mapsto (a+\mathfrak{p})/(u+\mathfrak{p})$. This is well-defined and surjective, since $u + \mathfrak{p} \neq 0 + \mathfrak{p}$ if and only if $u \notin \mathfrak{p}$. And since $R/\mathfrak{p}$ is an integral domain we have $(a+\mathfrak{p})/(u+\mathfrak{p}) = (0+\mathfrak{p})/(1+\mathfrak{p})$ if and only if $a + \mathfrak{p} = 0 + \mathfrak{p}$ which is equivalent to $a \in \mathfrak{p}$ again. Thus the kernel of this epimorphism is just $\mathfrak{m}_\mathfrak{p}$ and hence it induces the isomorphism given. □

Proof of (2.139):
Let us begin with (a) $\implies$ (b): If the radical $\sqrt{\mathfrak{a}} = \mathfrak{m} \in \operatorname{Smax}(R)$ is a maximal ideal, then $\mathfrak{a}$ is a primary ideal, according to (2.90.(iii)) and $\sqrt{\mathfrak{a}} = \mathfrak{m}$ was a given. The next step is (b) $\implies$ (c): As $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$ is generally true and $\sqrt{\mathfrak{a}} = \mathfrak{m}$ is part of the assumption, we have $\mathfrak{a} \subseteq \mathfrak{m}$. Now consider any $\mathfrak{p} \in \operatorname{Spec}(R)$ with $\mathfrak{a} \subseteq \mathfrak{p} \subseteq \mathfrak{m}$. Then, as any prime ideal is radical, we clearly have $\mathfrak{m} = \sqrt{\mathfrak{a}} \subseteq \sqrt{\mathfrak{p}} = \mathfrak{p} \subseteq \mathfrak{m}$. From this we get $\mathfrak{p} = \mathfrak{m}$, which means that $\mathfrak{m}$ is minimal over $\mathfrak{a}$. Now for (c) $\implies$ (d): As $\mathfrak{a} \subseteq \mathfrak{m}$ and $\mathfrak{m}$ is a maximal (and hence prime) ideal, we have $\mathfrak{m} \in \mathbb{V}(\mathfrak{a})$. Conversely consider any $\mathfrak{p} \in \mathbb{V}(\mathfrak{a})$, that is $\mathfrak{p}$ is a prime ideal with $\mathfrak{a} \subseteq \mathfrak{p}$. As $\mathfrak{p} \neq R$ (any prime ideal is proper, by definition) there is a maximal ideal containing $\mathfrak{p}$, by (2.4.(ii)). But $\mathfrak{m}$ is the only prime ideal available, in R, as R was assumed to be a local ring. That is $\mathfrak{p} \subseteq \mathfrak{m}$. Together this is $\mathfrak{a} \subseteq \mathfrak{p} \subseteq \mathfrak{m}$ and by assumption (c) this is $\mathfrak{p} = \mathfrak{m}$. Therefore $\mathbb{V}(\mathfrak{a}) = \{\mathfrak{m}\}$. We finally go full circle, (d) $\implies$ (a): By (2.32) we have $\sqrt{\mathfrak{a}} = \mathbb{IV}(\mathfrak{a}) = \bigcap\{\mathfrak{m}\} = \mathfrak{m}$, just what we needed. □

Proof of (2.142):

(U) As $R \neq 0$ we have $1 \neq 0$ and hence by property (1) we find $\nu(1) \in \mathbb{N}$. Thus by (2) we get $\nu(1) = \nu(1 \cdot 1) = \nu(1) + \nu(1) \in \mathbb{Z}$. And together this implies $\nu(1) = 0$. Now consider any $\alpha \in R^*$ then by (2) again $0 = \nu(1) = \nu(\alpha\alpha^{-1}) = \nu(\alpha) + \nu(\alpha^{-1}) \geq \nu(\alpha) \geq 0$ hence $\nu(\alpha) = 0$.

(I) If we are given $a, b \in R$ with $ab = 0$ then by (1) and (2) we have $\infty = \nu(ab) = \nu(a) = \nu(b)$. Thus $\nu(a)$ and $\nu(b)$ may not both be finte and by (1) this means $a = 0$ or $b = 0$.

(P) First of all $0 \in [\nu]$ as by (1) we have $\nu(0) = \infty \geq 1$ and $1 \notin [\nu]$ as $\nu(1) = 0 < 1$ by (U). If now a, $b \in [\nu]$ and $c \in R$ then we compute

$$\begin{aligned} \nu(a+b) &\;\geq\; \min\{\,\nu(a), \nu(b)\,\} \;\geq\; 1 \\ \nu(ac) &\;=\; \nu(a) + \nu(c) \;\geq\; \nu(a) \;\geq\; 1 \end{aligned}$$

And hence $a + b$ and $ac \in [\nu]$ again. Hence $[\nu]$ truly is an ideal of R and $[\nu] \neq R$ as $1 \notin [\nu]$. Now suppose $ab \in [\nu]$ for some $a, b \in R$, that is $\nu(ab) = \nu(a) + \nu(b) \geq 1$. Then it cannot be that $\nu(a) = 0 = \nu(b)$ and hence $a \in [\nu]$ or $b \in [\nu]$, which means $[\nu]$ is prime.

(iii) It is clear that $1 \mid a$ for any $a \in R$ and hence $0 \in \{k \in \mathbb{N} \mid p^k \mid a\}$. Therefore $[a]_p \in \mathbb{N} \cup \{\infty\}$ is well-defined.

- As any $p^k \mid 0$ it is clear that $\nu(0) = \infty$. Conversely suppose that $\nu(a) = \infty$ for some $a \in R$. Then for any $k \in \mathbb{N}$ we may choose some $a_k \in R$ such that $a = p^k a_k$. Then $p^{k+1}a_{k+1} = a = p^k a_k$ and as R is an integral domain this implies $pa_{k+1} = a_k$, in particular $a_{k+1} \mid a_k$. Going to ideals this yields an ascending chain

$$a_0 S \subseteq a_1 S \subseteq \ldots \subseteq a_k S \subseteq \ldots$$

 As R is noetherian there is some $s \in \mathbb{N}$ such that $a_s R = a_{s+1} R$, i.e. there is some $\alpha \in R^*$ such that $a_{s+1} = \alpha a_s = \alpha p a_{s+1}$. If $a_{s+1} \neq 0$ this would mean $p = \alpha^{-1}$ (as R is an integral domain) which is absurd, since p is prime. Thus we have $a_{s+1} = 0$ and hence $a = p^{s+1}a_{s+1} = 0$.

- If $g = 0$ then $\nu(fg) = \infty = \nu(f) + \nu(g)$, thus we only need to consider $0 \neq f, g \in R$. Now write $f = p^k a$ and $g = p^l b$ where $k = [f]_p$ and $l = [g]_p$, then by maximality we have $p \nmid a$ and $p \nmid b$ and hence $p \nmid ab$, since p is prime. Hence $\nu(fg) = \nu(p^{k+l}ab) = k + l = \nu(f) + \nu(g)$.

- If $g = 0$ then $\nu(f+g) = \nu(f) = \min\{\nu(f), \nu(g)\}$, thus we only need to consider $0 \neq f, g \in R$. As above let us write $f = p^k a$ and $g = p^l b$ where $k = [f]_p$ and $l = [g]_p$. Without loss of generality we may assume $k \leq l$ then $f + g = p^k(a + p^{l-k}b)$ and hence $\nu(f+g) = \nu(p^k(a+p^{l-k}b)) = k + \nu(a + p^{l-k}b) \geq k = \min\{\nu(f), \nu(g)\}$. Thus by now ν is a valuation on R and it is normed, since $\nu(p) = 1$.

- Continuing with the previous item now prove the fifth property: i.e. we even have $k < l$. If we now had $p \mid a + p^{l-k}b$, then there would be some $h \in S$ such that $a = ph - p^{l-k}b$. But this would imply $p \mid a$ which is absurd, by maximality of k. Hence $\nu(f+g) = k = \min\{\nu(f), \nu(g)\}$.

(iv) $\nu \mapsto [\nu]$ is well-defined:
As ν is normed, we have $[\nu] \neq 0$. Hence $[\nu]$ is a non-zero-prime ideal, and as R is a PID this even implies maximality.

- $\mathfrak{m} \mapsto \nu_p$ is well-defined:
 If we have $pR = \mathfrak{m} = qR$ then there is some $\alpha \in R^*$ with $\alpha p = q$ and as $(\alpha p)^k \mid a \iff p^k \mid a$ we then also get $\nu_q = \nu_{\alpha p} = \nu_p$.

- $\mathfrak{m} \mapsto \nu_p \mapsto [\nu_p] = \mathfrak{m}$:
 It is clear that $[\nu_p] = pR$ and as also $\mathfrak{m} = pR$ by construction $[\nu_p] = \mathfrak{m}$.

- $\nu \mapsto [\nu] \mapsto \nu_p = \nu$:
 By construction we have $[\nu] = pR$, thus if $a \in R$ with $p \nmid a$ then $a \notin pR = [\nu]$ and hence $\nu(a) = 0$. And as ν is normed, there is some $q \in S$ such that $\nu(q) = 1$. Hence $q \in [\nu] = pR$, which means $p \mid q$. Therefore $1 \leq \nu(p)$ (as $p \in pR = [\nu]$) and $\nu(p) \leq \nu(q) = 1$ (as $p \mid q$) imply $\nu(p) = 1$. If now $f \in R$ is given aribtarily then we write $f = p^k a$ where $p \nmid a$, then $\nu(f) = k\nu(p) + \nu(a) = k = \nu_p(f)$. And hence $\nu = \nu_p$.

□

Proof of (2.146):

(i) The properties (1), (2) and (3) of valued rings and discrete valuation rings are identical. Hence it suffices to check that R is non-zero. But by (N) there is some $m \in R$ with $\nu(m) = 1 \neq \infty$ and by (1) this is $m \neq 0$. In particular $R \neq 0$.

(ii) We have already seen in (2.142.(i)) that $[\nu]$ is a prime ideal of R. Thus by (2.136) it suffices to check $R \setminus [\nu] \subseteq R^*$. Thus consider any $a \in R \setminus [\nu]$, that is $\nu(a) = 0 = \nu(1)$ and hence $\nu(1) \leq \nu(a)$ and $\nu(a) \leq \nu(1)$. By (4) this implies $1 \mid a$ and $a \mid 1$ which again is $a \approx 1$ or in other words $a \in R^*$.

(iii) By (i) and (2.142.(i)) we know that R is an integral domain. Thus consider $a, b \in R$ with $a \neq 0$, then we need to find some $q, r \in R$ such that $b = qa + r$ and ($r = 0$ or $\varepsilon(r) < \varepsilon(a)$). To do this we distinguish three cases: if $b = 0$, then we may choose $q := 0$ and $r := 0$. If $b \neq 0$ and $\nu(b) < \nu(a)$, then we may let $q := 0$ and $r := b$. Thus if $b \neq 0$ and $\nu(a) \leq \nu(b)$, then by (4) we get $a \mid b$. That is there is some $q \in R$ such that $b = qa$. Hence we are done by letting $r := 0$.

(iv) By induction on $k \in \mathbb{N}$ it is clear that $\nu(m^k) = k\nu(m) = k$. Thus for $\nu(a) = k = \nu(m^k)$ we obtain $a \mid m^k$ and $m^k \mid a$. That is $a \approx m^k$ are associates and hence there is some $\alpha \in R^*$ such that $a = \alpha m^k$. And the uniqueness of α is clear, as R is an integral domain.

(v) Let $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$ be any ideal of R, combining (iii) and (2.79.(iii)) we know that R is a PID. That is there is some $a \in R$ such that $\mathfrak{a} = aR$. In case $a = 0$ we have $\mathfrak{a} = 0$, else using (iv) we may write a as $a = \alpha m^k$ for some $\alpha \in R^*$. Thus we have $\mathfrak{a} = aR = \alpha m^k R = m^k R$ as claimed.

(vi) As $\nu(0) = \infty \geq 0$ and $\nu(1) = 0 \geq 0$ we have $0, 1 \in R$. Also we have $\nu(-1) = \nu((-1)(-1)) = 2\nu(-1)$ such that $\nu(-1) = 0$ and hence $-1 \in R$, too. If now $a, b \in R$ then by (3) we get $a + b \in R$ and by (2) also $ab \in R$. Altogether R is a sub-ring of F. We will now prove that ν is a discrete valuation on R again. Properties (1), (2), (3) and (N) are inherited trivially. And for (4) we are given $a, b \in R$ with $\nu(a) \leq \nu(b)$. In case $b = 0$ we have $a \cdot 0 = 0 = b$ and hence $a \mid b$ trivially. Thus assume $b \neq 0$, then we have $0 \leq \nu(a) \leq \nu(b) < \infty$ and hence $a \neq 0$, as well. Therefore we may let $x := ba^{-1} \in F$. Then by (2) we get $\nu(b) = \nu(xa) = \nu(x) + \nu(a)$, such that $\nu(x) = \nu(b) - \nu(a) \geq 0$. This again means $x \in R$ and hence $a \mid b$. It only remains to verify, that F truly is the quotient field of R. Thereby the inclusion " $\supseteq$ " is trivial. Hence consider any $x \in F$, if $\nu(x) \geq 0$ then $x = x \cdot 1^{-1}$ and we are done. Else we have $\nu(x^{-1}) = -\nu(x) > 0$ and hence $x^{-1} \in R$. Thus we likewise obtain $x = 1 \cdot (x^{-1})^{-1}$.

□

Proof of (2.147):

- (a) $\Longrightarrow$ (c): If (R, ν) is a discrete valuation ring, then R already is a local ring (with maximal ideal $[\nu]$) and an Euclidean ring, due to (2.146). But the latter implies that R is a PID, by (2.79.(iii)). And of course R cannot be a field, as there is some $m \in R$ with $\nu(m) = 1$ (and hence we have both $m \neq 0$ and $m \notin R^*$ as else $\nu(m) = 0$).

- (c) $\Longrightarrow$ (d): As R is a PID it is a UFD according to (2.79.(ii)). Now consider two prime elements $p, q \in R$, that is the ideals pR and qR are non-zero prime ideals. Hence - as R is a PID - pR and qR already are maximal by (2.79.(i)). But as R also is local this means $pR = qR$.

- (d) $\implies$ (b): Choose any $0 \neq n \in R \setminus R^*$ which is possible, as R is not a field. As R is an UFD we may choose some prime factor m of n and let $\mathfrak{m} := mR$. Now consider any $0 \neq a \in R$, as R is an UFD a admits a primary decomposition $a = \alpha p_1 \dots p_k$. But by assumption any prime factor p_i is associated to m, that is a admits the representation $a = \omega m^k$ for some $\omega \in R^*$ and $k \in \mathbb{N}$. If we had $a \notin R^*$ then we necessarily have $k \geq 1$ and hence $a \in mR = \mathfrak{m}$. Thus we have proved $R \setminus R^* \subseteq \mathfrak{m}$. And as $m \notin R^*$ we have $\mathfrak{m} \neq R$ such that R is a local ring with maximal ideal $\mathfrak{m}$, according to (2.136). And this again yields $R \setminus \mathfrak{m} = R^*$ as claimed. Now suppose $0 \neq a \in \bigcap_k m^k R$, as we have seen we may write $a = \omega m^k$ for some $\omega \in R^*$ and $k \in \mathbb{N}$. But by assumption on a we also have $a = bm^{k+1}$ for some $b \in R$. Dividing by m^k (R is an integral domain) we get $\omega = bm$ and hence $m \in R^*$ - a contradiction. Thus we also got $\bigcap_k m^k R = 0$.

- (b) $\implies$ (a): Let $\nu : R \to \mathbb{N} \cup \{\infty\} : a \mapsto \sup\{k \in \mathbb{N} \mid m^k \mid a\}$, then we will prove that ν is a discrete valuation on R: (1) if $a = 0$ then for any $k \in \mathbb{N}$ we clearly have $m^k \mid a$ and hence $\nu(0) = \infty$. Conversely if $\nu(a) = \infty$, then we have $m^k \mid a$ for any $k \in \mathbb{N}$ and hence $a \in \bigcap_k m^k R = 0$. (2) and (3) are easy by definition of ν - refer to the proof of (2.142.(ii)) for this. (4) Consider a and $b \in R$ with $\nu(a) \leq \nu(b)$. If $b = 0$ then $a \mid b$ is clear, otherwise we write $a = \alpha m^i$ and $b = \beta m^j$ for $i = \nu(a)$ and $j = \nu(b)$. By maximality of i we get $m \nmid \alpha$ and hence $\alpha \in R \setminus mR = R^*$. Thus we may define $h := \alpha^{-1}\beta m^{j-i}$ and thereby obtain $ha = b$ such that $a \mid b$. (N) suppose $m^2 \mid m$, then there was some $h \in R$ such that $hm^2 = m$ and hence $hm = 1$, which is $m \in R^*$. But in this case we had $R^* = R \setminus mR = \emptyset$ - a contradiction. Thus we have $\nu(m) \leq 1$ which clearly is $\nu(m) = 1$.

- (c) $\implies$ (f): Any PID is a noetherian UFD and by (2.65) an UFD is a normal ring. And the maximal ideal $\mathfrak{m}$ is non-zero, as we would else find $R^* = R \setminus \mathfrak{m} = R \setminus \{0\}$, which would mean that R was a field. Thus let $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ be any prime ideal of R, if $\mathfrak{p} \neq 0$ is non-zero, then $\mathfrak{p}$ already is maximal, due to (2.79.(i)). But in this case we necessarily have $\mathfrak{p} = \mathfrak{m}$, as R was assumed to be local.

- (f) $\implies$ (e): First of all $\mathfrak{m}$ is a finitely generated R-module, as R is a noetherian ring. Thus if we had $\mathfrak{m} = \mathfrak{m}^2 = \mathfrak{m}\,\mathfrak{m}$ then (as $\mathrm{JAC}(R) = \mathfrak{m}$) Nakayama's lemma (3.44) would imply $\mathfrak{m} = 0$ - a contradiction. Thus we have $\mathfrak{m}^2 \subset \mathfrak{m}$, that is there is some $m \in \mathfrak{m}$ with $m \notin \mathfrak{m}^2$. In what follows we will prove $\mathfrak{m} = mR$. (1) First note that $m \neq 0$ (as else $m \in \mathfrak{m}^2$), thus by assumption and (2.25.(i)) we get

$$\sqrt{mR} \;=\; \bigcap \{\, \mathfrak{p} \in \mathrm{Spec}(R) \mid mR \subseteq \mathfrak{p} \,\} \;=\; \mathfrak{m}$$

 In particular $\mathfrak{m} \subseteq \sqrt{mR}$ and hence there is some $k \in \mathbb{N}$ such that $\mathfrak{m}^k \subseteq mR$, by (2.25.(vii)). And of course we may choose k minimal with this property (that is $\mathfrak{m}^{k-1} \not\subseteq mR$). Clearly $k = 0$ cannot occur (as $m \in \mathfrak{m}$ and hence m is not a unit of R). And if $k = 1$ we are done, as in this case we get $\mathfrak{m} \subseteq mR \subseteq \mathfrak{m}$. Thus in the following we will assume $k \geq 2$ and derive a contradiction. (2) by minimality of k there is some $a \in \mathfrak{m}^{k-1}$ with $a \notin mR$. Let $a\mathfrak{m} := \{ab \mid b \in \mathfrak{m}\}$, as $a \in \mathfrak{m}^{k-1}$ we have $a\mathfrak{m} \subseteq \mathfrak{m}^{k-1}\mathfrak{m} = \mathfrak{m}^k \subseteq mR$. Now let $x := a/m \in E$, where $E := \mathrm{QUOT}(R)$ is the quotient field of R. Then clearly $x \notin R$ (that is $m \nmid a$) as else $a \in mR$ in contradiction to the choice of a. (3) Now it is easy to see that $x\mathfrak{m} := \{xb \mid b \in \mathfrak{m}\}$ is a subset $x\mathfrak{m} \subseteq R$ of R: for any $b \in \mathfrak{m}$ we have $xb = ab/m \in (1/m)\,mR = R$. And in fact $x\mathfrak{m}$ even is an ideal $x\mathfrak{m} \trianglelefteq_{\mathrm{i}} R$ of R ($0 \in x\mathfrak{m}$ is clear, and obviously $x\mathfrak{m}$ is closed under $+$, $-$ and multiplication with elements of R). Now by construction we even get $x\mathfrak{m} \neq R$ (as else there would be some $b \in \mathfrak{m}$ such that $xb = 1$. But this

would imply $m = ab \in a\mathfrak{m} \subseteq \mathfrak{m}^k \subseteq \mathfrak{m}^2$ (as we assumed $k \geq 2$) in contradiction to the choice of m). Thus $x\mathfrak{m}$ is a proper ideal of R and as R is a local ring with maximal ideal $\mathfrak{m}$ this implies $x\mathfrak{m} \subseteq \mathfrak{m}$. (4) Let us now choose generators of $\mathfrak{m}$, say $\mathfrak{m} = b_1R + \cdots + b_nR$. As $x\mathfrak{m} \subseteq \mathfrak{m}$ there are coefficients $a_{i,j} \in R$ (where $j \in 1 \ldots n$) such that for any $i \in 1 \ldots n$

$$xb_i \;=\; a_{i,1}b_1 + \cdots + a_{i,n}b_n$$

Let us now define $b := (b_1, \ldots, b_n)$ and the $n \times n$ matrix $A := (a_{i,j})$ over R. Then the above equations can be reformulated as $Ab = xb$, that is $b \in \ker(x\mathbb{1} - A)$. Thereby $(x\mathbb{1} - A)$ is a $n \times n$ matrix over the field E and as it has a kernel we have $\det(x\mathbb{1} - A) = 0 \in E$. Thus if $f := \det(t\mathbb{1} - A) \in R[t]$ is the characteristic polynomial of A then we have $f(x) = \det(x\mathbb{1} - A) = 0$. But as R was assumed to be normal and as f is a normed polynomial over R, this implies $x = a/m \in R$ or in other words $a \in mR$, a contradiction. This contradiction can only be solved in case $k = 1$ and then we have already seen $\mathfrak{m} = mR$.

- (e) $\Longrightarrow$ (c): First of all R is not a field, as $\mathfrak{m}$ is a proper non-trivial ideal of R (that is $0 \neq \mathfrak{m} \neq R$). It remains to verify, that R is a PID, where $\mathfrak{m} = mR$ was assumed to be a principal ideal. To do this we first let $\mathfrak{z} := \bigcap_k \mathfrak{m}^k \trianglelefteq_{\mathrm{i}} R$, as R is noetherian $\mathfrak{z}$ is a finitely generated R-module. And further we have $\mathfrak{m}\mathfrak{z} = \mathfrak{z}$ ("$\subseteq$" is clear and conversely if $a \in \mathfrak{z}$ then for any $k \in \mathbb{N}$ there is some $h_k \in R$ such that $a = h_k m^k$. Therefore $a/m = h_{k+1}m^k$ for any $k \in \mathbb{N}$ and hence $a/m \in \mathfrak{z}$ which is $a \in \mathfrak{m}\mathfrak{z}$ again). As $\mathfrak{m} = \mathrm{JAC}(R)$ the lemma of Nakayama (3.44) implies that $\mathfrak{z} = 0$. We now define the following map

$$\nu \;:\; \trianglelefteq_{\mathrm{i}} R \to \mathbb{N} \cup \{\infty\} \;:\; \mathfrak{a} \mapsto \sup\Big\{\, k \in \mathbb{N} \mid \mathfrak{a} \subseteq \mathfrak{m}^k \,\Big\}$$

Obviously ν is well defined, as $\mathfrak{a} \subseteq R = \mathfrak{m}^0$ for any $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$. And if $\mathfrak{a} \neq R$, then $\mathfrak{a}$ is contained in some maximal ideal, which is $\mathfrak{a} \subseteq \mathfrak{m}$ and hence $\nu(\mathfrak{a}) \geq 1$. Now suppose $\nu(\mathfrak{a}) = \infty$, this means $\mathfrak{a} \subseteq \bigcap_k \mathfrak{m}^k = 0$ and hence $\mathfrak{a} = 0$. Of course both 0 and R are principal ideals. Thus consider any ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ with $0 \neq \mathfrak{a} \neq R$. As we have just seen, this yields $1 \leq k := \nu(\mathfrak{a}) \in \mathbb{N}$. And as $\mathfrak{a} \not\subseteq \mathfrak{m}^{k+1}$ we may choose some $a \in \mathfrak{a}$ with $a \notin \mathfrak{m}^{k+1}$. As $\mathfrak{a} \subseteq \mathfrak{m}^k$ we in particular have $a \in \mathfrak{m}^k$, that is $a = \alpha m^k$ for some $\alpha \in R$. If we had $\alpha \in \mathfrak{m}$ then $a \in \mathfrak{m}^{k+1}$ would yield a contradiction. Hence $\alpha \in R \setminus \mathfrak{m} = R^*$ is a unit. Therefore we found $\mathfrak{m}^k = m^kR = \alpha m^kR = aR \subseteq \mathfrak{a} \subseteq \mathfrak{m}^k$ and hence $\mathfrak{a} = m^kR$ is a principal ideal. Altogether R is a PID.

□

Proof of (2.150):

(i) By definition of a local ring it suffices to check $R \setminus R^* \trianglelefteq_{\mathrm{i}} R$. As $R \neq 0$ we have $0 \in R \setminus R^*$. Now consider any $a, b \in R \setminus R^*$ and $r \in R$. Then $ra \in R \setminus R^*$, as else $a^{-1} = r(ar)^{-1}$ and in particular $-a \in R \setminus R^*$. It remains to show that $a + b \in R \setminus R^*$. Without loss of generality we may assume $a \mid b$ (else we may interchange a and b). That is $b = ab$ for some $h \in R$ and hence $a + b = a(1 + h)$. Thus we have $a + b \in R \setminus R^*$, as else $a^{-1} = (1 + h)(a + b)^{-1}$.

(i) By assumption R is an integral domain. Thus regard any finitely generated ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$. That is there are $a_1, \ldots, a_k \in R$ (where we may choose k minimally) such that $\mathfrak{a} = a_1R + \cdots + a_kR$. We

need to show that $\mathfrak{a}$ is a principal ideal, that is $k = 1$. Thus assume $k \neq 1$, then $\mathfrak{a} \neq a_1 R$ (as k is minimal) and hence there is some $b \in \mathfrak{a}$ such that $b \notin a_1 R$. Now write $b = a_1 b_1 + \cdots + a_k b_k$ and let $d := a_2 b_2 + \cdots + a_k b_k$. If we had $a_1 \mid d$ then $d \in a_1 R$ and hence $b = a_1 b_1 + d \in a_1 R$, a contradiction. Thus we have $d \mid a_1$ as R is a valuation ring. But this means $a_1 \in dR \subseteq a_2 R + \cdots + a_k R$ and hence $\mathfrak{a} = a_1 R + \cdots + a_k R = a_2 R + \cdots + a_k R$ in contradiction to the minimality of k. This only leaves $k = 1$ which had to be shown.

(ii) (c) $\Longrightarrow$ (b) is true by (2.146.(iii)) and (b) $\Longrightarrow$ (a) is clear. Thus it remains to verify (a) $\Longrightarrow$ (c): as R is a valuation ring, it is a Bezout domain, by (i). Thus if R also is noetherian it clearly is a PID. But R also is local by (i) and a local PID is a field or a DVR by (2.147).

□

Proof of (2.153):
It is clear that $\mathfrak{f} + \mathfrak{g}$, $\mathfrak{f} \cap \mathfrak{g}$ and $\mathfrak{f}\mathfrak{g}$ are R-sub-modules again. If now $r\mathfrak{f} \subseteq R$ and $s\mathfrak{g} \subseteq R$ then we can also check property (2) of fraction ideals

$$\begin{array}{rcccl} (rs)(\mathfrak{f}+\mathfrak{g}) & = & s(r\mathfrak{f}) + r(s\mathfrak{g}) & \subseteq & R \\ r(\mathfrak{f}\cap\mathfrak{g}) & \subseteq & r\mathfrak{f} & \subseteq & R \\ (rs)(\mathfrak{f}\mathfrak{g}) & = & (r\mathfrak{f})\,(s\mathfrak{g}) & \subseteq & R \end{array}$$

Further $\mathfrak{f} : \mathfrak{g}$ is an R-sub-module of F since: if $x, y \in \mathfrak{f} : \mathfrak{g}$ and $a \in R$ then $(ax + y)\mathfrak{g} \subseteq a\mathfrak{f} + \mathfrak{f} = \mathfrak{f}$. Thus it remains to prove that $\mathfrak{f} : \mathfrak{g} \trianglelefteq_{\mathfrak{f}} R$ truly is a fraction ideal. To do this let $r\mathfrak{f} \subseteq R$ and $s\mathfrak{g} \subseteq R$. As $\mathfrak{g} \neq 0$ we may choose some $0 \neq g \in \mathfrak{g}$, then clearly $sg \in \mathfrak{g} \cap R$ and $sg \neq 0$, as R is an integral domain. But now $(rsg)(\mathfrak{f} : \mathfrak{g}) \subseteq R$ as for any $x \in \mathfrak{f} : \mathfrak{g}$ we get$(rsg)x = r(xsg) \in r\mathfrak{f} \subseteq R$. □

Proof of (2.155):
(b) $\Longrightarrow$ (a) is trivial, by choosing $\mathfrak{g} := R : \mathfrak{f}$. Thus consider (a) $\Longrightarrow$ (b): that is we assume $\mathfrak{f}\mathfrak{g} = R$ for some $\mathfrak{g} \trianglelefteq_{\mathfrak{f}} R$. Then by construction we have $\mathfrak{g} \subseteq \{x \in F \mid x\mathfrak{f} \subseteq R\} = R : \mathfrak{f}$. Hence $R = \mathfrak{f}\mathfrak{g} \subseteq \mathfrak{f}(R : \mathfrak{f}) \subseteq R$ (the latter inclusion has been shown in the remark above) which is $R = \mathfrak{f}(R : \mathfrak{f})$. It remains to verify the uniqueness of the inverse $\mathfrak{g}$ - but this is simply due to the associativity of the multiplication. We start with $\mathfrak{f}\mathfrak{g} = R = \mathfrak{f}(R : \mathfrak{f})$. Multiplying (from the left) with $\mathfrak{g}$ yields $\mathfrak{g} = R\mathfrak{g} = (\mathfrak{f}\mathfrak{g})\mathfrak{g} = (\mathfrak{g}\mathfrak{f})\mathfrak{g} = \mathfrak{g}(\mathfrak{f}\mathfrak{g}) = \mathfrak{g}(\mathfrak{f}(R : \mathfrak{f})) = (\mathfrak{g}\mathfrak{f})(R : \mathfrak{f}) = (\mathfrak{f}\mathfrak{g})(R : \mathfrak{f}) = R(R : \mathfrak{f}) = R : \mathfrak{f}$. □

Proof of (2.156):
(a) $\Longrightarrow$ (b): by assumption (a) we've got $1 \in R = \mathfrak{a}\mathfrak{g}$. Hence there are some $a_i \in \mathfrak{a}$ and $x_i \in \mathfrak{g}$ such that $1 = a_1 x_1 + \ldots a_n x_n \in \mathfrak{a}\mathfrak{g}$. And as the x_i are contained in $x_i \in \mathfrak{g} = \mathfrak{a}^{-1} = R : \mathfrak{a}$ we have $x_i\mathfrak{a} \in R$ as claimed. (b) $\Longrightarrow$ (a): conversely suppose we are given such a_i and x_i then by definition $a_i \in \mathfrak{a}$ and $x_i \in R : \mathfrak{a}$. And as $a_1 x_1 + \ldots a_n x_n = 1$ we also we have $R \subseteq \mathfrak{a}(R : \mathfrak{a}) \subseteq R$ and hence $R = \mathfrak{a}(R : \mathfrak{a})$. Thus we next concern ourselves with the implication (b) $\Longrightarrow$ (c): suppose we have chosen some $a_i \in \mathfrak{a}$ and $x_i \in F$ as noted under (b), then we define two R-module homomorphisms

$$\psi \;:\; R^n \to \mathfrak{a} \;:\; (r_1, \ldots, r_n) \mapsto a_1 r_1 + \ldots a_n r_n$$

$$\psi' \;:\; \mathfrak{a} \to R^n \;:\; a \mapsto (ax_1, \ldots, ax_n)$$

Note that the latter is well-defined, since $x_i\mathfrak{a} \subseteq R$ by assumption. But if now $a \in \mathfrak{a}$ is chosen arbitarily

then we get

$$\psi\psi'(a) \;=\; aa_1x_1 + \cdots + aa_nx_n \;=\; a$$

as $a_1x_1 + \cdots + a_nx_n = 1$. This is $\psi\psi' = \mathbb{1}$ on $\mathfrak{a}$. Now regard the following (obviously exact) chain of R-modules

$$0 \longrightarrow \mathrm{kn}(\psi) \xrightarrow{\subseteq} R^n \xrightarrow{\psi} \mathfrak{a} \longrightarrow 0$$

As we have just seen, this chain splits, as $\psi\psi' = \mathbb{1}$ and hence $\mathfrak{a}$ is a direct summand of the free R-module R^n (which in particular means that $\mathfrak{a}$ is projective) by virtue of

$$R^n \;\cong_{\mathrm{m}}\; \mathfrak{a} \oplus \mathrm{kn}(\psi) \;:\; r \mapsto \Big(\psi(r), r - \psi'\psi(r)\Big)$$

Conversely suppose (c), that is $M = \mathfrak{a} \oplus P$, then we need to prove (b). To do this we define the R-module homomorphisms $\varrho : M \twoheadrightarrow \mathfrak{a} : (a,p) \mapsto a$ and $\iota : \mathfrak{a} \hookrightarrow M : a \mapsto (a,0)$. Then clearly $\varrho\,\iota = \mathbb{1}$. As M is free by assumption it has an R-basis $\{\, m_i \mid i \in I \,\}$. And hence any $a \in \mathfrak{a}$ has a representation in the form

$$a \;=\; \varrho\iota(a) \;=\; \varrho\left(\sum_{i\in I} a_i m_i\right) \;=\; \sum_{i\in I} a_i \varrho(m_i)$$

Note that only finitely many of the a_i are non-zero, as these are the coefficients of the basis representation of $\iota(a)$. This representation allows us to define another R-module homomorphism

$$\pi_i \;:\; \mathfrak{a} \to R \;:\; a \mapsto a_i$$

Now consider any two non-zero elements $0 \neq a, b \in \mathfrak{a}$ then we see that $b\pi_i(a) = \pi_i(ba) = \pi_i(ab) = a\pi_i(b)$. And hence we may define an element $x_i \in F$ independently of the choice of $0 \neq a \in \mathfrak{a}$ by letting

$$x_i \;:=\; \frac{\pi_i(a)}{a}$$

Note that only finitely many a_i were non-zero and hence only finitely many x_i are non-zero. The one property is easy to see: if $0 \neq a \in \mathfrak{a}$ is any element then we get $x_i a = \pi_i(a) \in R$ and hence $x_i\mathfrak{a} \subseteq R$. The other property requires only slightly more effort: just compute

$$a \;=\; \sum_{i\in I} \pi_i(a)\varrho(m_i) \;=\; \sum_{i\in I} a x_i \varrho(m_i) \;=\; a\left(\sum_{i\in I} x_i \varrho(m_i)\right)$$

Recall that only finitely many x_i were non-zero and for these let us denote $h_i := \varrho(m_i)$. As a was non-zero we may divide by a to see that $1 = \sum_i x_i h_i$ which was all that remained to prove. □

Proof of (2.157):

- (a) $\Longrightarrow$ (b): as $\mathfrak{a} \neq 0$ is non-zero $a \neq 0$ is non-zero and hence we may choose $\mathfrak{g} := (1/a)R$. Then we clearly get $\mathfrak{a}\,\mathfrak{g} = (aR)(1/aR) = R$.
- (b) $\Longrightarrow$ (a): as $\mathfrak{a}$ is invertible, it is a projective R-module. But R is a local ring and hence any projective R-module already is free. Now $\mathfrak{a}$ being free implies that $\mathfrak{a}$ is a principal ideal (if the basis contained more than one element - say b_1 and b_2 - then $b_2b_1 + (-b_1)b_2 = 0$ would be a non-trivial linear combination).

□

Proof of (2.159):
We will now prove the equivalences in the definition of Dedekind domains. Among other useful statements we will thereby proof (2.161.(i)) already. Note that the order of proofs is somewhat unusual: (d) $\iff$ (e) followed by (e) $\implies$ (a) $\implies$ (b) $\implies$ (c) $\implies$ (b) $\implies$ (d).

- (d) $\implies$ (e): consider any prime ideal $\mathfrak{q} \trianglelefteq_{\mathrm{i}} R$ and let $U := R \setminus \mathfrak{q}$, that is $R_{\mathfrak{q}} = U^{-1}R$. Then $R_{\mathfrak{q}}$ is a local ring by (2.138). And as R was assumed to be normal, so is $R_{\mathfrak{q}}$, by (2.131). And by (2.129) the spectrum of $R_{\mathfrak{q}}$ corresponds to $\{\, \mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \subseteq \mathfrak{q} \,\}$. Yet if $\mathfrak{p} \neq 0$, then $\mathfrak{p}$ already is maximal by assumption and hence $\mathfrak{p} = \mathfrak{q}$. Thus we have $\{\, \mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \subseteq \mathfrak{q} \,\} = \{\, 0, \mathfrak{q} \,\}$. Thereby $\mathrm{Spec}(R_{\mathfrak{q}})$ has precisely the prime ideals 0 (corresponding to 0 in R) and its maximal ideal (corresponding to $\mathfrak{q}$) in R. Altogether it satisfies condition (f) of DVRs.

- (e) $\implies$ (d): by assumption R is a noetherian integral domain. Thus it remains to prove, that it is normal and satisfies $\mathrm{Spec}(R) = \mathrm{Smax}(R) \cap \{0\}$. By assumption any localization $R_{\mathfrak{p}}$ is a DVR, hence a PID, hence an UFD and hence normal by (2.65). And as R is an integral domain this implies that R itself is normal, too by (2.134). Thus consider any prime ideal $0 \neq \mathfrak{p} \trianglelefteq_{\mathrm{i}} R$. It remains to prove that $\mathfrak{p}$ is maximal. Thus we choose any maximal ideal ideal $\mathfrak{m}$ with $\mathfrak{p} \subseteq \mathfrak{m}$. By assumption $R_{\mathfrak{m}}$ is a DVR, and hence has precisely the prime ideals 0 and $\mathfrak{m}_{\mathfrak{m}}$ (2.147). But as $0 \neq \mathfrak{p} \subseteq \mathfrak{m}$ by (2.129) the localization $\mathfrak{p}_{\mathfrak{m}}$ is a non-zero prime ideal of $R_{\mathfrak{m}}$ and hence $\mathfrak{p}_{\mathfrak{m}} = \mathfrak{m}_{\mathfrak{m}}$. Invoking the correspondence again we find $\mathfrak{p} = \mathfrak{m}$ and hence $\mathfrak{p}$ truly is maximal.

- R DVR $\implies$ (a): let $\mathfrak{m}$ be the maximal ideal of R and m a uniformizing parameter, that is $\mathfrak{m} = mR$. (1) If now $0 \neq \mathfrak{f} \trianglelefteq_{\mathrm{f}} R$ is a non-zero fraction ideal, then $\mathfrak{a} := \mathfrak{f} \cap R \trianglelefteq_{\mathrm{i}} R$ is an ideal of R. And by definition there is some $0 \neq r \in R$ such that $r\mathfrak{f} \subseteq R$. Recall that by (2.146.(iv)) in a DVR $r \in R$ is uniquely represented, as $r = \varrho m^k$ with $\varrho \in R^*$ and $k = \nu(r) \in \mathbb{N}$. Among those $r \in R$ with $r\mathfrak{f} \subseteq R$ we now choose one with minimal $k = \nu(r)$. (2) We first note that $\mathfrak{a} \neq 0$, just choose some $0 \neq x \in \mathfrak{f}$, then $rx \in \mathfrak{a}$ and as $r, x \neq 0$ we also have $rx \neq 0$. Thus by (2.146.(v)) $\mathfrak{a}$ is of the form $\mathfrak{a} = m^n R$ for some $n \in \mathbb{N}$. (3) Now
$$\mathfrak{f} \;=\; m^{n-k} R$$
"$\subseteq$" if $x \in \mathfrak{f}$ then by (2) we have $rx \in \mathfrak{a} = m^n R$, say $rx = m^n p$. Therefore $x = m^n p/r = \varrho^{-1} p m^{n-k} \in m^{n-k}R$. "$\supseteq$" If $k = 0$, then $r = \varrho \in R^*$ is a unit and hence $\mathfrak{f} = r\mathfrak{f} \subseteq R$. Thus we get $\mathfrak{f} = \mathfrak{a} = m^n R = m^{n-k}R$. Now suppose $k \geq 1$, as k has been chosen minimally, there is some $x = a/b \in \mathfrak{f}$ such that $m^{k-1}x \notin R$. That is $b \not| m^{k-1}a$ and hence $\nu(b) > \nu(m^{k-1}a) = k - 1 + \nu(a)$ by the properties of discrete valuations. However $rx \in R$ and hence $b \mid m^k a$. This yields $\nu(b) \leq \nu(am^k) = k + \nu(a)$ altogether $\nu(b) = k + \nu(a)$. Thus if we represent $a = \alpha m^i$ with $\alpha \in R^*$ and $i = \nu(a)$ then $b = \beta m^j$ with $\beta \in R^*$ and $j = \nu(b) = k + i$. Therefore $x = a/b = \alpha\beta^{-1}m^{-k}$ such that $rx = \alpha\varrho\beta^{-1} \in R^*$. On the other hand $rx \in \mathfrak{a} = m^n R$ and hence $\mathfrak{a} = R$, that is $n = 0$. Thus $m^{-k} = \beta\alpha^{-1}x \in \mathfrak{f}$ such that $m^{n-k}R = m^{-k}R \subseteq \mathfrak{f}$. This settles the proof of the equality (3). But now we have seen, that $\mathfrak{f} = m^{n-k}R$ is a principal ideal, in particular it is invertible, with inverse $\mathfrak{f}^{-1} = m^{k-n}R$.

- (e) $\implies$ (a): if R is a field, then $\mathfrak{f} = R$ is the one and only non-zero fraction ideal of R. And $\mathfrak{f} = R$ trivially is invertible, with inverse $\mathfrak{f}^{-1} = R$. Thus in the following we assume that R is not

a field, then we choose any non-zero prime ideal $0 \neq \mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ in R and let $U := R \setminus \mathfrak{p}$. That is $U^{-1}R = R_{\mathfrak{p}}$ and by assumption $R_{\mathfrak{p}}$ is a DVR. Thus consider a non-zero fraction ideal $0 \neq \mathfrak{f} \trianglelefteq_{\mathrm{f}} R$, then $0 \neq U^{-1}\mathfrak{f} \trianglelefteq_{\mathrm{f}} R_{\mathfrak{p}}$ is a fraction ideal of $R_{\mathfrak{p}}$. But as we have just seen this implies, that $U^{-1}R$ is invertible (regarding $R_{\mathfrak{p}}$). But by the remarks in section 2.12 this already yields that $\mathfrak{f}$ is invertible (regarding R).

- (a) $\implies$ (b) is trivial, so we will now prove (b) $\implies$ (c): by assumption (b) any non-zero ideal is invertible and hence finitely generated (by the remarks in section 2.12). And as 0 trivially is finitely generated R is a noetherian ring. Now consider any non-trivial ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$, that is $\mathfrak{a} \notin \{0, R\}$ and let $\mathfrak{a}_0 := \mathfrak{a}$. As $\mathfrak{a} \neq R$ we may choose some prime ideal $\mathfrak{p}_1 \in \operatorname{Spec}(R)$ containing $\mathfrak{a} \subseteq \mathfrak{p}_1$, by (2.4.(ii)). Now let

$$\mathfrak{a}_1 \;:=\; \mathfrak{a}_0(\mathfrak{p}_1)^{-1} \;=\; \mathfrak{a}_0(R:\mathfrak{p}_1) \;\subseteq\; \mathfrak{a}_0(R:\mathfrak{a}_0) \;=\; R$$

 Here the inclusion $R:\mathfrak{p}_1 \subseteq R:\mathfrak{a}_0$ holds because of $\mathfrak{a}_0 \subseteq \mathfrak{p}_1$ and $\mathfrak{a}_0(R:\mathfrak{a}_0) = R$ is true because $\mathfrak{a}_0$ is invertible by assumption (a). Hence $\mathfrak{a}_1 \trianglelefteq_{\mathrm{i}} R$ is an ideal of R and by construction

$$\mathfrak{a} \;=\; \mathfrak{a}_0 \;=\; \mathfrak{p}_1\mathfrak{a}_1$$

 We will now construct an ascending chain $\mathfrak{a} = \mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \ldots \subseteq \mathfrak{a}_n \ldots$ of ideals of R. Suppose we have already constructed $\mathfrak{a}_k \trianglelefteq_{\mathrm{i}} R$ and the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_k \in \operatorname{Spec}(R)$ such that $\mathfrak{a} = \mathfrak{p}_1 \ldots \mathfrak{p}_k\mathfrak{a}_k$. If $\mathfrak{a}_k = R$ then we are done as we have already decomposed $\mathfrak{a} = \mathfrak{p}_1 \ldots \mathfrak{p}_k$ in this case. Thus assume $\mathfrak{a}_k \neq R$. Then we may choose any prime ideal $\mathfrak{p}_{k+1}$ containing $\mathfrak{a}_k \subseteq \mathfrak{p}_{k+1}$ again. As for the case $k = 1$ above, we let $\mathfrak{a}_{k+1} := \mathfrak{a}_k(\mathfrak{p}_{k+1})^{-1}$ and find that $\mathfrak{a}_{k+1} \trianglelefteq_{\mathrm{i}} R$ is an ideal of R. Then by construction we get

$$\mathfrak{a} \;=\; \mathfrak{p}_1 \ldots \mathfrak{p}_k\,\mathfrak{a}_k \;=\; \mathfrak{p}_1 \ldots \mathfrak{p}_k\,\mathfrak{p}_{k+1}\,\mathfrak{a}_{k+1}$$

 As R is noetherian this chain stabilizes at some point $\mathfrak{a}_n = \mathfrak{a}_{n+1}$ and by construction this means $\mathfrak{a}_{n+1} = \mathfrak{a}_n = \mathfrak{p}_{n+1}\mathfrak{a}_{n+1}$. As $\mathfrak{a}_{n+1}$ is a finitely generated R-module the lemma of Dedekind implies that there is some $p \in \mathfrak{p}_{n+1}$ such that $(1-p)\mathfrak{a}_{n+1} = 0$. But as R is an integral domain and $\mathfrak{a}_{n+1} \neq 0$ this means that $p = 1$, which is absurd, since $\mathfrak{p}_{n+1} \neq R$ is prime. Thus the construction fails at this stage, which can only be if $\mathfrak{a}_n = R$. And as we have mentioned already this is $\mathfrak{a} = \mathfrak{p}_1 \ldots \mathfrak{p}_n$.

- (b) $\implies$ (2.161.(i)): the existence of the factorisation of non-trivial ideals into prime non-zero ideals has been shown in (b) $\implies$ (c) already. Hence it only remains to show that the factorisation is unique up to permutations. Thus assume $\mathfrak{p}_1 \ldots \mathfrak{p}_m = \mathfrak{q}_1 \ldots \mathfrak{q}_n$ where $0 \neq \mathfrak{p}_i$ and $\mathfrak{q}_j \trianglelefteq_{\mathrm{i}} R$ are non-zero prime ideals. Whithout loss of generality we assume $m \leq n$ and use induction on n. The case $m = 1 = n$ is trivial so we are only concerned with the induction step: by renumbering we may assume that $\mathfrak{q}_1$ is minimal among $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_n\}$. And as

$$\mathfrak{p}_1 \ldots \mathfrak{p}_m \;\subseteq\; \bigcap_{i=1}^{m} \mathfrak{p}_i \;\subseteq\; \mathfrak{q}_1$$

 and $\mathfrak{q}_1$ is prime (2.14.(ii)) implies that there is some $i \in 1 \ldots m$ such that $\mathfrak{p}_i \subseteq \mathfrak{q}_1$. Now conversely

as $\mathfrak{p}_i$ is prime and $\mathfrak{q}_1 \dots \mathfrak{q}_n \subseteq \mathfrak{p}_i$ there is some $j \in 1 \dots n$ such that $\mathfrak{q}_j \subseteq \mathfrak{p}_i \subseteq \mathfrak{q}_1$. By minimality of $\mathfrak{q}_1$ this means $\mathfrak{q}_j = \mathfrak{q}_1$ and hence $\mathfrak{p}_i = \mathfrak{q}_1$. By renumbering we may assume $i = 1$. Then multiplying by $\mathfrak{p}_1^{-1} = \mathfrak{q}_1^{-1}$ yields $\mathfrak{p}_2 \dots \mathfrak{p}_m = \mathfrak{q}_2 \dots \mathfrak{q}_n$ so we are done by the induction hypothesis.

- (c) $\implies$ any invertible prime ideal is maximal. Thus consider some invertible prime ideal $\mathfrak{p} \trianglelefteq_{\mathfrak{i}} R$, in particular $\mathfrak{p} \neq 0$. We will show that for any $u \in R \setminus \mathfrak{p}$ we get $\mathfrak{p} + uR = R$. Suppose we had $\mathfrak{p} + uR \neq R$ then by (b) we could decompose $\mathfrak{p} + uR = \mathfrak{p}_1 \dots \mathfrak{p}_m$ for some prime ideals $\mathfrak{p}_i \trianglelefteq_{\mathfrak{i}} R$. Now take to the quotient ring $R/\mathfrak{p}$, then by (1.66)

$$0 \neq (u+\mathfrak{p})^R\big/_{\mathfrak{p}} = \mathfrak{p}+uR\big/_{\mathfrak{p}} = \mathfrak{p}_1\big/_{\mathfrak{p}} \dots \mathfrak{p}_m\big/_{\mathfrak{p}}$$

But $(u+\mathfrak{p})(R/\mathfrak{p})$, being a principal ideal, is invertible. In particular any of its factors $\mathfrak{p}_i/\mathfrak{p}$ is invertible with inverse given to be

$$\left(\mathfrak{p}_i\big/_{\mathfrak{p}}\right)^{-1} = \left(\frac{1}{u+\mathfrak{p}}\, R\big/_{\mathfrak{p}}\right)\left(\prod_{i\neq j}\mathfrak{p}_j\big/_{\mathfrak{p}}\right)$$

Now we open up a second line of argumentation: we decompose the ideal $\mathfrak{p} + u^2R = \mathfrak{q}_1 \dots \mathfrak{q}_n$ and take to the quotient ring again

$$0 \neq (u^2+\mathfrak{p})^R\big/_{\mathfrak{p}} = \mathfrak{p}+u^2R\big/_{\mathfrak{p}} = \mathfrak{q}_1\big/_{\mathfrak{p}} \dots \mathfrak{q}_n\big/_{\mathfrak{p}}$$

As $((u+\mathfrak{p})R/\mathfrak{p})^2 = (u^2+\mathfrak{p})R/\mathfrak{p}$ we have found two decompositions of $(u^2+\mathfrak{p})R/\mathfrak{p}$ into prime ideals - to be precise we found

$$\left(\mathfrak{p}_1\big/_{\mathfrak{p}}\right)^2 \dots \left(\mathfrak{p}_m\big/_{\mathfrak{p}}\right)^2 = \mathfrak{q}_1\big/_{\mathfrak{p}} \dots \mathfrak{q}_n\big/_{\mathfrak{p}}$$

$R/\mathfrak{p}$ also satisfies the assumption (c) because of the correspondence theorem and as any $\mathfrak{p}_i/\mathfrak{p}$ is invertible the decomposition is unique up to permutations - note that these truly are the only assumptions that were used in the proof of (iii). Hence (by the uniqueness) we get $2m = n$ and $(\mathfrak{p}_1/\mathfrak{p}, \mathfrak{p}_1/\mathfrak{p}, \dots, \mathfrak{p}_m/\mathfrak{p}, \mathfrak{p}_m/\mathfrak{p}) \longleftrightarrow (\mathfrak{q}_1/\mathfrak{p}, \dots, \mathfrak{q}_n/\mathfrak{p})$. But by the correspondence theorem (1.66) again we can return to the original ring R getting $(\mathfrak{p}_1, \mathfrak{p}_1 \dots, \mathfrak{p}_m, \mathfrak{p}_m) \longleftrightarrow (\mathfrak{q}_1, \dots, \mathfrak{q}_n)$. Therefore

$$\begin{aligned} \mathfrak{p} + u^2R &= \mathfrak{q}_1 \dots \mathfrak{q}_n \\ &= \mathfrak{p}_1\mathfrak{p}_1 \dots \mathfrak{p}_m\mathfrak{p}_m \\ &= (\mathfrak{p}+uR)^2 \\ &= \mathfrak{p}^2 + u\mathfrak{p} + u^2R \end{aligned}$$

Hence $\mathfrak{p} \subseteq \mathfrak{p} + u^2R = \mathfrak{p}^2 + u(\mathfrak{p}+uR) \subseteq \mathfrak{p}^2 + uR$. Thus any $p \in \mathfrak{p}$ has a representation as $p = a + ub$ where $a \in \mathfrak{p}^2$ and $b \in R$. Thus $ub = p - a \in \mathfrak{p}$ such that $b \in \mathfrak{p}$. This is $p = a + ub \in \mathfrak{p}^2 + u\mathfrak{p}$ and as p has been arbitrary $\mathfrak{p} \subseteq \mathfrak{p}^2 + u\mathfrak{p} = \mathfrak{p}(\mathfrak{p}+uR)$. Multiplying with $\mathfrak{p}^{-1}$ this is $R \subseteq \mathfrak{p} + uR$ and hence finally $\mathfrak{p} + uR = R$.

- (c) $\implies$ (b): we will first show that non-zero prime ideals $0 \neq \mathfrak{p} \trianglelefteq_{\mathfrak{i}} R$ are invertible. To do this choose some $0 \neq a \in \mathfrak{p}$ and decompose $aR = \mathfrak{p}_1 \dots \mathfrak{p}_n$. As aR is invertible - with inverse

$(aR)^{-1} = (1/a)R$ - any $\mathfrak{p}_i$ is invertible, as its inverse is just

$$\left(\mathfrak{p}_i\right)^{-1} \;=\; \frac{1}{a}R \prod_{i\neq j} \mathfrak{p}_j$$

As $\mathfrak{p}$ is prime and $\mathfrak{p}_1 \ldots \mathfrak{p}_n = aR \subseteq \mathfrak{p}$ there is some $i \in 1 \ldots n$ such that $\mathfrak{p}_i \subseteq \mathfrak{p}$. But $\mathfrak{p}_i$ is invertible and hence maximal (see above) such that $\mathfrak{p}_i = \mathfrak{p}$. Thus $\mathfrak{p}$ is invertible. If now $0 \neq \mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$ is any non-zero ideal then we decompose $\mathfrak{a} = \mathfrak{p}_1 \ldots \mathfrak{p}_n$ and as any $\mathfrak{p}_i$ is now known to be irreducible we have $\mathfrak{a}^{-1} = \mathfrak{p}_1^{-1} \ldots \mathfrak{p}_n^{-1}$ invertible.

- (b) $\iff$ (c) and (b) $\implies \mathrm{Spec}(R) = \mathrm{Smax}(R) \cup \{0\}$. We have just established the equivalence (b) $\iff$ (c). And we have seen above that (because of (c)) any invertible prime ideal is maximal. But because of (b) *any* non-zero prime ideal already is invertible and hence maximal.

- (b) $\implies$ (d): we have already seen - in (b) $\implies$ (c) - that R is noetherian and that $\mathrm{Spec}(R) = \mathrm{Smax}(R) \cup \{0\}$. Thus it only remains to show that R is normal. If R is a field already then there is nothing to prove, else let $F := \mathrm{QUOT}(R)$ and regard $x = a/b \in F$. If x is integral over R then $R[x]$ is an R-module of finite rank $k+1 := \mathrm{rank}R[x]$. Let now $r := b^k$ - as any element of $R[x]$ is of the form $a_k x^k + \cdots + a_1 x + a_0$ (for some $a_i \in R$) we clearly have $rR[x] \subseteq R$ (in particular $R[x] \trianglelefteq_{\mathfrak{f}} R$ is a fraction ideal of R). And hence for any $n \in \mathbb{N}$ we have $s_n := rx^n \in R$. For any prime ideal $\mathfrak{p} \trianglelefteq_{\mathfrak{i}} R$ let us now denote by $\nu_{\mathfrak{p}}(\mathfrak{a})$ the multiplicity of $\mathfrak{p}$ in the primary decomposition of $\mathfrak{a}$, i.e. we let

$$\nu_{\mathfrak{p}}(\mathfrak{p}_1 \ldots \mathfrak{p}_m) \;:=\; \#\{\, i \in 1 \ldots m \mid \mathfrak{p} = \mathfrak{p}_i \,\} \;\in\; \mathbb{N}$$

Then clearly $\nu_{\mathfrak{p}}$ turns the multiplication of ideals into an addition of multiplicities and hence $ra^n = s_n b^n$ turns into

$$\nu_{\mathfrak{p}}(rR) + n\nu_{\mathfrak{p}}(aR) \;=\; \nu_{\mathfrak{p}}(s_n R) + n\nu_{\mathfrak{p}}(bR)$$

Hence for any $n \in \mathbb{N}$ and any prime ideal $\mathfrak{p} \trianglelefteq_{\mathfrak{i}} R$ we get the estimate

$$\nu_{\mathfrak{p}}(rR) + n(\nu_{\mathfrak{p}}(aR) - \nu_{\mathfrak{p}}(bR)) \;\geq\; \nu_{\mathfrak{p}}(s_n R) \;\geq\; 0$$

By choosing $n > \nu_{\mathfrak{p}}(rR)$ this implies that for any prime ideal $\mathfrak{p}$ we have $\nu_{\mathfrak{p}}(bR) \leq \nu_{\mathfrak{p}}(aR)$. Writing down decompositions of aR and bR we hence find that $aR \subseteq bR$. But this is $b \mid a$ or in other words $x \in R$ which had to be shown.

□

Proof of (2.163):
The proof of the equivalences in the definition (2.162) and the properties (2.163) of valuations of ideals in Dedekind domains is interwoven tightly. Thus we do not attempt to give separate proofs, but verify the properties and equivalences simultaneously.

- $\mathfrak{b} \mid \mathfrak{a} \iff \mathfrak{a} \subseteq \mathfrak{b}$: if $\mathfrak{a} = \mathfrak{b}\,\mathfrak{c}$, then $\mathfrak{b} \subseteq \mathfrak{a}$ is clear. Conversely suppose we had $\mathfrak{a} \subseteq \mathfrak{b}$. If additionally $\mathfrak{b} = 0$ then $\mathfrak{a} = 0$, too and hence we may already take $\mathfrak{c} := R$. Thus suppose $\mathfrak{b} \neq 0$ and let $\mathfrak{c} := \mathfrak{b}^{-1}\mathfrak{a} \trianglelefteq_{\mathfrak{f}} R$. Then $\mathfrak{c} \subseteq \mathfrak{b}^{-1}\mathfrak{b} = R$ and hence $\mathfrak{c} = \mathfrak{c} \cap R \trianglelefteq_{\mathfrak{i}} R$. But on the other hand $\mathfrak{b}\,\mathfrak{c} = \mathfrak{b}\,\mathfrak{b}^{-1}\mathfrak{a} = \mathfrak{a}$ is clear, such that $\mathfrak{b} \mid \mathfrak{a}$.

(i) In case $\mathfrak{m} \notin \mathcal{M}$ we may pick up $\mathfrak{m}_0 := \mathfrak{m}$ and $k(0) := 0$ reducing this to to the case $\mathfrak{m} \in \mathcal{M}$. And if $\mathfrak{m} \in \mathcal{M}$ then by renumbering we may assume that $\mathfrak{m} = \mathfrak{m}_1$. Thus regard $\mathfrak{a} := \mathfrak{m}_1^{k(1)} \dots \mathfrak{m}_n^{k(n)}$, then $\mathfrak{a} \subseteq \mathfrak{m}^{k(1)}$ is clear and hence $\nu_{\mathfrak{m}}(\mathfrak{a}) \geq k(1)$, by definition of $\nu_{\mathfrak{m}}$. Thus assume $\nu_{\mathfrak{m}} > k(1)$, this means $\mathfrak{a} \subseteq \mathfrak{m}^{k(1)+1}$ and by what we have just shown there is some $\mathfrak{c} \trianglelefteq_{\mathfrak{i}} R$ such that $\mathfrak{a} = \mathfrak{m}^{k(1)+1}\mathfrak{c}$. Therefore

$$\mathfrak{m}_1^{k(2)} \dots \mathfrak{m}_n^{k(n)} \;=\; \mathfrak{m}^{-k(1)}\mathfrak{a} \;=\; \mathfrak{m}\,\mathfrak{c} \;\subseteq\; \mathfrak{m}$$

But as $\mathfrak{m}$ is prime this means that there is some $i \in 2 \dots n$ such that $\mathfrak{m}_i^{k(i)} \subseteq \mathfrak{m}$. Clearly $k(i) \neq 0$ as else $R \subseteq \mathfrak{m}$ and hence $\mathfrak{m}_i \subseteq \mathfrak{m}$ by the same argument. But $\mathfrak{m}_i$ has been maximal and hence $\mathfrak{m}_i = \mathfrak{m} = \mathfrak{m}_1$ in contradiction to the $\mathfrak{m}_i$ being pairwise distinct.

(ii) Decompose $\mathfrak{a} = \mathfrak{m}_1^{k(1)} \dots \mathfrak{m}_n^{k(n)}$ and $\mathfrak{b} = \mathfrak{m}_1^{l(1)} \dots \mathfrak{m}_n^{l(n)}$ as in the formulation of (iii). Also as in the proof of (i) we may also assume that $\mathfrak{m} = \mathfrak{m}_1$ (by picking up $\mathfrak{m}_0 := \mathfrak{m}$, $k(0) := 0$ and $l(0) := 0$ if necessary and renumbering). Then it is clear that $\mathfrak{a}\,\mathfrak{b} = \mathfrak{m}_1^{k(1)+l()} \dots \mathfrak{m}_n^{k(n)+l(n)}$. And using (i) the claim follows readily: $\nu_{\mathfrak{m}}(\mathfrak{a}\,\mathfrak{b}) = k(1) + l(1) = \nu_{\mathfrak{m}}(\mathfrak{a}) + \nu_{\mathfrak{m}}(\mathfrak{b})$.

- $\mathfrak{a} \mid \mathfrak{b} \iff \forall\, \mathfrak{m} : \nu_{\mathfrak{m}}(\mathfrak{b}) \leq \nu_{\mathfrak{m}}(\mathfrak{a})$. Clearly if $\mathfrak{a} = \mathfrak{b}\,\mathfrak{c}$ then by (ii) we get $\nu_{\mathfrak{m}}(\mathfrak{a}) = \nu_{\mathfrak{m}}(\mathfrak{b}) + \nu_{\mathfrak{m}}(\mathfrak{b}) \geq \nu_{\mathfrak{m}}(\mathfrak{b})$. Conversely decompose $\mathfrak{a} = \mathfrak{m}_1^{k(1)} \dots \mathfrak{m}_n^{k(n)}$ and $\mathfrak{b} = \mathfrak{m}_1^{l(1)} \dots \mathfrak{m}_n^{l(n)}$ once more. By (i) that is $k(i) = \nu_{\mathfrak{m}_i}(\mathfrak{a})$ and $l(i) = \nu_{\mathfrak{m}_i}(\mathfrak{b})$. Thus by assumption we have $l(i) \leq k(i)$ and may hence define $\mathfrak{c} = \mathfrak{m}_1^{k(1)-l(1)} \dots \mathfrak{m}_n^{k(n)-l(1)} \trianglelefteq_{\mathfrak{i}} R$. Then by construction we immediately get $\mathfrak{b}\,\mathfrak{c} = \mathfrak{a}$.

(iii) First let $m(\mathfrak{m}) := \min\{\, \nu_{\mathfrak{m}}(\mathfrak{a}), \nu_{\mathfrak{m}}(\mathfrak{b}) \,\}$ for any $\mathfrak{m} \in \mathrm{Smax}(R)$. Note that for $\mathfrak{m} = \mathfrak{m}_i$ we in particular get $m(\mathfrak{m}) = m(i)$ and if $\mathfrak{m}$ is not contained in the $\mathfrak{m}_i$ then $m(\mathfrak{m}) = 0$. And therefore we get

$$\mathfrak{m}_1^{m(1)} \dots \mathfrak{m}_n^{m(n)} \;=\; \prod_{\mathfrak{m}} \mathfrak{m}^{m(\mathfrak{m})}$$

Now consider any ideal $\mathfrak{c} \trianglelefteq_{\mathfrak{i}} R$, then by the equivalences we have already proved for $\mathfrak{a} \mid \mathfrak{b}$ it is evident that we obtain the following chain of equivalent statements

$$\begin{aligned}
& \forall\, \mathfrak{m} \;:\; \nu_{\mathfrak{m}}(\mathfrak{c}) \leq \nu_{\mathfrak{m}}(\mathfrak{a}+\mathfrak{b}) \\
\iff\; & \mathfrak{a}+\mathfrak{b} \;\subseteq\; \mathfrak{c} \\
\iff\; & \mathfrak{a} \subseteq \mathfrak{c} \text{ and } \mathfrak{b} \subseteq \mathfrak{c} \\
\iff\; & \forall\, \mathfrak{m} \;:\; \nu_{\mathfrak{m}}(\mathfrak{c}) \leq \nu_{\mathfrak{m}}(\mathfrak{a}) \quad \text{and} \quad \nu_{\mathfrak{m}}(\mathfrak{c}) \leq \nu_{\mathfrak{m}}(\mathfrak{b}) \\
\iff\; & \forall\, \mathfrak{m} \;:\; \nu_{\mathfrak{m}}(\mathfrak{c}) \leq m(\mathfrak{m})
\end{aligned}$$

Thus for a fixed $\mathfrak{m} \in \mathrm{Smax}(R)$ we may regard $\mathfrak{c} := \mathfrak{m}^j$. And by (i) this satisfies $\nu_{\mathfrak{m}}(\mathfrak{c}) = j$, that is we may take $\nu_{\mathfrak{m}}(\mathfrak{c})$ to be any $j \in \mathbb{N}$ of our liking. And therefore the above equivalence immediately yields $\nu_{\mathfrak{m}}(\mathfrak{a}+\mathfrak{b}) = m(\mathfrak{m})$ and hence the equality for $\mathfrak{a}+\mathfrak{b}$ claimed.

(iv) Consider any two non-zero ideals $\mathfrak{a}$, $\mathfrak{b}$ of R, then by (iii) $\mathfrak{a}$ and $\mathfrak{b}$ are coprime (i.e. $\mathfrak{a}+\mathfrak{b} = R$) if and only if for any $\mathfrak{m} \in \mathrm{Smax}(R)$ we get $\nu_{\mathfrak{m}}(\mathfrak{a}) = 0$ or $\nu_{\mathfrak{m}}(\mathfrak{b}) = 0$. In particular for any $\mathfrak{m} \neq \mathfrak{m} \in \mathrm{Smax}(R)$ and any k, $l \in \mathbb{N}$ we see that $\mathfrak{m}^k$ and $\mathfrak{n}^l$ are coprime. Thus the claim follows immediately from the original Chinese remainder theorem (1.99).

(v) If $\mathfrak{a} = aR$ is a principal ideal, then we may take $\mathfrak{b} := R$, then $\mathfrak{a}+\mathfrak{b} = R$ and $\mathfrak{a}\,\mathfrak{b} = \mathfrak{a} = aR$ are satisfied trivially. Thus suppose $\mathfrak{a}$ is no principal ideal (in particular $\mathfrak{a} \neq 0$), then we may

decompose $\mathfrak{a} = \mathfrak{m}_1^{k(1)} \dots \mathfrak{m}_n^{k(n)}$ as usual. Now for any $i \in 1 \dots n$ pick up some $b_i \in R$ such that $b_i \in \mathfrak{m}_i^{k(i)}$ but $b_i \notin \mathfrak{m}_i^{k(i)+1}$ (thereby $\mathfrak{m}_i^{k(i)} \setminus \mathfrak{m}_i^{k(i)+1} \neq \emptyset$ is non-empty, as we else had $R = \mathfrak{m}_i$ by multiplication with $\mathfrak{m}_i^{-k(i)}$). Hence by (iv) there is some $b \in R$ that is mapped to $(b_i \in \mathfrak{m}_i^{k(i)+1})$ under the isomorphism of the Chinese remainder theorem. That is for any $i \in 1 \dots n$ we have $b + \mathfrak{m}_i^{k(i)+1} = b_i + \mathfrak{m}_i^{k(i)+1}$. In particular we find $b \in \mathfrak{m}_i^{k(i)}$ and $b \notin \mathfrak{m}_i^{k(i)+1}$ again. This is to say that $\nu_{\mathfrak{m}_i}(b) = k_i$ for any $i \in 1 \dots n$. That is if we decompose bR then there are some $n \leq N \in \mathbb{N}$, $\mathfrak{m}_i \in \mathrm{Smax}(R)$ and $1 \leq k(i) \in \mathbb{N}$ (where $i \in n+1 \dots N$) such that

$$bR \;=\; \prod_{\mathfrak{m}} \mathfrak{m}^{k(\mathfrak{m})} \;=\; \prod_{i=1}^{N} \mathfrak{m}_i^{k(i)}$$

Note that $n < N$, if we had $n = N$ then $bR = \mathfrak{a}$ already would be a principal ideal, which had been dealt with already. Thus if we let $\mathfrak{b} := \mathfrak{m}_{n+1}^{k(n+1)} \dots \mathfrak{m}_N^{k(N)}$, then it is evident, that $\mathfrak{a}\,\mathfrak{b} = bR$ is principal. But also by construction $\mathfrak{a}$ and $\mathfrak{b}$ satisfy $\nu_{\mathfrak{m}}(\mathfrak{a}) = 0$ or $\nu_{\mathfrak{m}}(\mathfrak{b}) = 0$ for any $\mathfrak{m} \in \mathrm{Smax}(R)$. And as we have already argued in (iv) this is $\mathfrak{a} + \mathfrak{b} = R$.

□

Proof of (2.161):
Note that (i) and (ii) have already been shown while proving the equivalences in the definition of Dedekind domains on page 1111. Thus it only remains to verify (iii) to (vi), which we will do now:

(vi) Let us denote the mapping (of course we still have to check the well-definedness) given by Φ, that is $\Phi(a + \mathfrak{m}^k) := a/1 + \mathfrak{m}^k R_{\mathfrak{m}}$. Now consider any a, $b \in R$ and u, $v \notin \mathfrak{m}$, then in a first step, we will prove

$$\frac{a}{u} + \mathfrak{m}^k R_{\mathfrak{m}} + \frac{b}{v} + \mathfrak{m}^k R_{\mathfrak{m}} \quad\Longleftrightarrow\quad av - bu \in \mathfrak{m}^k$$

If $av - bu \in \mathfrak{m}^k$ then (as $uv \notin \mathfrak{m}$) it is clear, that $(a/u) - (b/v) = (av - bu)/uv \in \mathfrak{m}^k R_{\mathfrak{m}}$. And thereby also $a/u + \mathfrak{m}^k R_{\mathfrak{m}} + b/v + \mathfrak{m}^k R_{\mathfrak{m}}$. Conversely let us assume $(av - bu)/uv = (a/u) - (b/v) \in \mathfrak{m}^k R_{\mathfrak{m}}$. That is there are some $m \in \mathfrak{m}^k$ and $w \notin \mathfrak{m}$ such that $(av - bu)/uv = m/w$ and hence $w(av - bu) = muv \in \mathfrak{m}^k$. Therefore $w(av - bu)R \subseteq \mathfrak{m}^k$ such that by (2.162) and (2.163)

$$k \;=\; \nu_{\mathfrak{m}}(\mathfrak{m}^k) \;\leq\; \nu_{\mathfrak{m}}(w(av - bu)) \;=\; \nu_{\mathfrak{m}}(w) + \nu_{\mathfrak{m}}(av - bu)$$

Yet $w \notin \mathfrak{m}$ and hence $\nu_{\mathfrak{m}}(w) = 0$. Therefore we get $\nu_{\mathfrak{m}}(av - bu) = k$ and this translates into $av - bu \in \mathfrak{m}^k$ as claimed. And this immediately yields the equivalences: $a + \mathfrak{m}^k = b + \mathfrak{m}^k$ iff $a - b \in \mathfrak{m}^k$ iff $\Phi(a + \mathfrak{m}^k) = \Phi(b + \mathfrak{m}^k)$. And this has been the well-definedness and injectivity of Φ. Thus it remains to prove the surjectivity of Φ: we are given any $a/u + \mathfrak{m}^k R_{\mathfrak{m}}$ and need to find some $b \in R$ such that $a/u + \mathfrak{m}^k R_{\mathfrak{m}} = b/1 + \mathfrak{m}^k R_{\mathfrak{m}}$. Yet $u \notin \mathfrak{m}$ and $\mathfrak{m}$ is a maximal ideal, that is $R/\mathfrak{m}$ is a field and hence there is some $v \notin \mathfrak{m}$ such that $v + \mathfrak{m} = (u + \mathfrak{m})^{-1}$. That is $1 - uv \in \mathfrak{m}$ and in particular $(1 - uv)^k \in \mathfrak{m}^k$. But by the binomial rule we may compute

$$\begin{aligned}(1 - uv)^k \;&=\; (-1)^k (uv - 1)^k \;=\; (-1)^k \sum_{i=0}^{k} \binom{k}{i} (uv)^i (-1)^{k-i} \\ &=\; \sum_{i=0}^{k} (-1)^i \binom{k}{i} (uv)^i \;=\; 1 + u \sum_{i=1}^{k} (-1)^i \binom{k}{i} u^{i-1} v^i\end{aligned}$$

That is we get $(1-uv)^k = 1+uq$ for some adequately chosen $q \in R$. Then we define $b := -aq$, now an easy computation yields $a - bu = a(1+uq) = a(1-uv)^k \in \mathfrak{m}^k$. Thus by the above equivalence we find $\Phi(b+\mathfrak{m}^k) = a/u + \mathfrak{m}^k R_\mathfrak{m}$.

(iii) (1) Let us first assume, that $\mathfrak{a} = \mathfrak{m}^k$ is a power of a maximal ideal $\mathfrak{m} \trianglelefteq_\mathrm{i} R$. If $k = 0$, then $\mathfrak{a} = R$ such that $R/\mathfrak{a} = 0$ such that we have nothing to prove. Thus assume $k \geq 1$, then by (vi) $R/\mathfrak{a}$ is isomorphic to $R_\mathfrak{m}/\mathfrak{a}R_\mathfrak{m}$. But as R is a Dedekind domain $R_\mathfrak{m}$ is a DVR (by (2.159.(e))) and in particular a PID (by (2.147.(c))). Therefore the quotient $R_\mathfrak{m}/\mathfrak{a}R_\mathfrak{m}$ is a principal ring (see section 2.7). Thus the isomorphy shows, that $R/\mathfrak{a}$ is a principal ring. (2) Now consider any $0 \neq \mathfrak{a} \trianglelefteq_\mathrm{i} R$. We have already dealt with the case $\mathfrak{a} = R$ in (1).($k = 0$). Thus suppose $\mathfrak{a} \neq R$ and decompose $\mathfrak{a} = \mathfrak{m}_1^{k(1)} \dots \mathfrak{m}_n^{k(n)}$ (with $n(i) \geq 1$). Then by the Chinese remainder theorem in (2.163)

$$R \Big/ \mathfrak{a} \quad \cong_\mathrm{r} \quad R \Big/ \mathfrak{m}_1^{k(1)} \oplus \dots \oplus R \Big/ \mathfrak{m}_n^{k(n)}$$

Now every $R/\mathfrak{m}_i^{k(i)}$ is a principal ring due to case (1). But the direct sum of principal rings is a principal again, due to the some remark in section 2.7. Thus the isomorphy shows, that $R/\mathfrak{a}$ is a principal ring.

(iv) Consider any $\mathfrak{a} \trianglelefteq_\mathrm{i} R$ and $0 \neq a \in R$, then by (iii) R/aR is a principal ring and hence $\mathfrak{a}/aR$ is a principal ideal - say $\mathfrak{a}/aR = (b+aR)(R/aR)$ for some $b \in R$. As $b + aR \in \mathfrak{a}/aR$ it is clear that $b \in \mathfrak{a}$, in particular $aR + bR \subseteq \mathfrak{a}$. Now consider any $c \in \mathfrak{a}$, then $c + aR \in \mathfrak{a}/aR = (b+aR)(R/aR)$. That is there is some $v \in R$ such that $c + aR = (b+aR)(v+aR) = bv + aR$. Hence $c - bv \in aR$ which means that $c - bv = au$ for some $u \in R$. And as $c = au + bv \in \mathfrak{a}$ has been arbitrary this also is $\mathfrak{a} \subseteq aR + bR$

(v) Let us denote the set of all prime ideals that are not principal by $\mathcal{P}$ - formally $\mathcal{P} := \{ \mathfrak{p} \in \mathrm{Spec}(R) \mid \nexists p \in R : \mathfrak{p} =$ (1) clearly $n := \#\mathcal{P} < \infty$, as $\mathcal{P} \subseteq \mathrm{Spec}(R) \setminus \{0\} = \mathrm{Smax}(R)$ and the maximal spectrum of R is finite by assumption. If we have $n = 0$ then any prime ideal is principal. Thus if $\mathfrak{a} \trianglelefteq_\mathrm{i} R$ is any ideal decompose $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_k$ where $\mathfrak{p}_i \trianglelefteq_\mathrm{i} R$ is prime (using (c)). Then $\mathfrak{p}_i = p_i R$ is principal and hence $\mathfrak{a} = aR$ is principal, too by letting $a := p_1 \dots p_k$. Thus it suffices to assume $n \geq 1$ and to derive a contradiction. (2) Let us denote $\mathfrak{b} := \mathfrak{p}_1 \dots \mathfrak{p}_n$ and $\mathfrak{a} := \mathfrak{p}_1 \mathfrak{b} = \mathfrak{p}_1^2 \mathfrak{p}_2 \dots \mathfrak{p}_n$. Then $\mathfrak{a} \neq \mathfrak{b}$, as else $R = \mathfrak{b}\,\mathfrak{b}^{-1} = \mathfrak{a}\,\mathfrak{b}^{-1} = \mathfrak{p}_1$ - a contradiction (recall that $\mathfrak{b} \neq 0$, as R is an integral domain and hence we may apply (b)). (3) Next we claim that there is some $u \in \mathfrak{p}_1$ such that $u \notin \mathfrak{p}_1^2$, $u \notin \mathfrak{p}_i$ for any $i \in 2 \dots n$ and $\mathfrak{p}_1 = \mathfrak{a} + uR$. In fact $\mathfrak{a} \neq 0$, as R is an integral domain and hence $R/\mathfrak{a}$ is a principal ring by (ii). And as $\mathfrak{p}_1/\mathfrak{a}$ is an ideal of $R/\mathfrak{a}$, there is some $u \in R$ such that

$$\mathfrak{p}_1 \Big/ \mathfrak{a} \;=\; (u+\mathfrak{a})^R \Big/ \mathfrak{a} \;=\; \mathfrak{a} + uR \Big/ \mathfrak{a}$$

By the correspondence theorem we find $\mathfrak{p}_1 = \mathfrak{a} + uR$ as $\mathfrak{a} \subseteq \mathfrak{p}_1$. Thus suppose $u \in \mathfrak{p}_1^2$, then $\mathfrak{p} = \mathfrak{a} + uR \subseteq \mathfrak{p}_1^2 \subseteq \mathfrak{p}_1$ and hence $\mathfrak{p}_1 = \mathfrak{p}_1^2$. Dividing by $\mathfrak{p}_1$ we would find $R = \mathfrak{p}_1$, a contradiction. And if we suppose $u \in \mathfrak{p}_i$ then likewise $\mathfrak{p}_1 = \mathfrak{a} + uR \subseteq \mathfrak{p}_i$. But as $\mathfrak{p}_1$ already is maximal this would imply $\mathfrak{p}_1 = \mathfrak{p}_i$ a contradiction (to $i \neq 1$). (4) now we prove that $uR = \mathfrak{p}_1 \mathfrak{q}_1 \dots \mathfrak{q}_m$ for some prime ideals $\mathfrak{q}_j \notin \mathcal{P}$. First of all uR admits a decomposition $uR = \mathfrak{q}_0 \dots \mathfrak{q}_m$ according to (b). Then $\mathfrak{q}_0 \dots \mathfrak{q}_m = uR \subseteq \mathfrak{p}_1$ and hence $\mathfrak{q}_0 \subseteq \mathfrak{p}_1$ for some $j \in 0 \dots m$, as $\mathfrak{p}_1$ is prime. Without loss of generality we may assume $j = 0$. Then $\mathfrak{q}_0 \subseteq \mathfrak{p}_1$ and this means $\mathfrak{q}_0 = \mathfrak{p}_1$, as $\mathfrak{q}_0$ is maximal (it

is non-zero, prime). Thus we have established the decomposition $uR = \mathfrak{p}_1\mathfrak{q}_1\dots\mathfrak{q}_m$, now assume $\mathfrak{q}_j \in \mathcal{P}$ for some $j \in 1\dots m$. If we had $\mathfrak{q}_j = \mathfrak{p}_i$ for some $i \in 2\dots n$ then $u \in uR \subseteq \mathfrak{p}_1$ in contradiction to (3). And if we had $\mathfrak{q}_j = \mathfrak{p}_1$ then $u \in uR \subseteq \mathfrak{p}_1^2$ in contradiction to (3) again. (5) Thus the $\mathfrak{q}_j \notin \mathcal{P}$ are principal ideals, say $\mathfrak{q}_j = q_jR$. Then we let $q := q_1\dots q_m$ and thereby find $uR = \mathfrak{p}_1\mathfrak{q}_1\dots\mathfrak{q}_m = \mathfrak{p}_1(qR)$. Thus $uR \subseteq qR$, say $u = qv$ for some $v \in R$. Then dividing by qR we find $\mathfrak{p}_1 = (u/q)R = vR$ such that $\mathfrak{p}_1 \in \mathcal{P}$ - a contradiciton at last.

□

Proof of (2.79):
It remains to prove statement (iv) of (2.79), as parts (i), (ii) and (iii) have already been proved on page 1054. So by assumption every prime ideal $\mathfrak{p}$ of R is generated by *one* element $\mathfrak{p} = pR$. In particular any prime ideal $\mathfrak{p}$ is generated by *finitely many* elements. Thus R is notherian by property (d) in (2.34). Further $0 \neq \mathfrak{p} = pR$ implies p to be prime by (2.58.(ii)) (and as R is an integral domain this also means that p is irreducible due to (2.58.(v))). In particular any nonzero prime ideal $0 \neq \mathfrak{p} \trianglelefteq_{\mathfrak{i}} R$ contains a prime element $p \in \mathfrak{p}$ (namely p with $\mathfrak{p} = pR$). And thus R is an UFD according to property (e) in (2.60). And by (2.65) this implies that R even is a normal domain. Now regard a non-zero prime ideal $0 \neq \mathfrak{p} = pR \trianglelefteq_{\mathfrak{i}} R$ again and suppose $\mathfrak{p} \subseteq \mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$ for some ideal $\mathfrak{a}$ of R. If $\mathfrak{a} \neq R$ then $\mathfrak{a}$ is contained in some maximal ideal $\mathfrak{a} \subseteq \mathfrak{m} \trianglelefteq_{\mathfrak{i}} R$ of R. And as any maximal ideal $\mathfrak{m}$ is prime, by assumption there is some $m \in R$ such that $\mathfrak{m} = mR$. Now $pR = \mathfrak{p} \subseteq \mathfrak{a} \subseteq \mathfrak{m} = mR$ implies $m \mid p$. That is there is some $q \in R$ such that $qm = p$. But as p is irreducible, this implies $q \in R^*$ (as $m \in R^*$ would imply $\mathfrak{m} = R$). That is $p \approx m$ and hence $\mathfrak{p} = \mathfrak{m}$ such that $\mathfrak{p} = \mathfrak{a}$, as well. This mean that $\mathfrak{p}$ already is a maximal ideal of R. Altogether we have proved, that R is a normal, noetherian domain in which any non-zero prime ideal is maximal. But this means that R is a Dedekind domain according to (c) in (2.159). Now consider any ideal $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$. Then due to (b) (2.159) there are prime ideals $\mathfrak{p}_1,\dots,\mathfrak{p}_n \trianglelefteq_{\mathfrak{i}} R$ such that $\mathfrak{a} = \mathfrak{p}_1\dots\mathfrak{p}_n$. By assumption there are $p_i \in R$ such that $\mathfrak{p}_i = p_iR$ and hence $\mathfrak{a} = (p_1R)\dots(p_nR) = (p_1\dots p_n)R$ is a principal ideal, too. As $\mathfrak{a}$ has been arbitrary, this finally means that R is a PID. □

Proof of (3.142):
As in the definition of the tensor product let us denote $X := M_1 \times \dots \times M_n$. Let us first define the map $\widetilde{\varphi}$ from $R^{\oplus X}$ to N, by virtue of

$$\widetilde{\varphi} \;:\; \sum_{x\in X} a_x e_x \mapsto \sum_{x\in X} a_x \varphi(x)$$

From this definition it is clear, that $\widetilde{\varphi}$ is a homomorphism of R-modules (as it has been defined, by linear expansion of $e_x \mapsto \varphi(x)$). Also recall the definition of T to be the sub-module generated by the elements $s(i,x,a)$ and $a(i,x,y_i)$. As φ is R-multilinear we get

$$\begin{aligned}
\widetilde{\varphi}(s(i,x,a)) &= a\varphi(x_1,\dots,x_i,\dots,x_n) - \varphi(x_1,\dots,ax_i,\dots,x_n)\\
&= 0\\
\widetilde{\varphi}(a(i,x,y_i)) &= \varphi(x_1,\dots,y_i,\dots,x_n) + \varphi(x_1,\dots,y_i,\dots,x_n)\\
&\quad -\varphi(x_1,\dots,x_i+y_i,\dots,x_n)\\
&= 0
\end{aligned}$$

where we denoted $x = (x_1,\dots,x_n)$. As T is generated by these elements, we get $\widetilde{\varphi}(t) = 0$ for any $t \in T$

and that is $T \subseteq \mathrm{kn}(\varphi)$. Hence $\widetilde{\varphi}$ induces a map $\overline{\varphi}$ of the form

$$\overline{\varphi} \ : \ {R^{\oplus X}}\Big/{T} \to N \ : \ \sum_{x\in X} a_x e_x + T \mapsto \sum_{x\in X} a_x \varphi(x)$$

As this is the tensor product $M_1 \otimes \ldots \otimes M_n = R^{\oplus X}/T$ (and $x_1 \otimes \ldots \otimes x_n = e_x + T$) this is the *existence* of the homomorphism $\overline{\varphi}$. It remains to prove its *uniqueness*: That is we consider some R-linear map $\psi : M_1 \otimes \ldots \otimes M_n \to N$ such that $\varphi = \psi\tau$. That is for any $x_j \in M_j$ (where $j \in 1 \ldots n$) we get

$$\varphi(x_1, \ldots, x_n) \ = \ \psi(x_1 \otimes \ldots \otimes x_n)$$

but as $M_1 \otimes \ldots \otimes M_n$ is generated by the elements of the form $x_1 \otimes \ldots \otimes x_n$ and ψ and $\overline{\varphi}$ have to coincide on these elements this already implies $\psi = \overline{\varphi}$.
So we have proved the well-definedness of $\varphi \mapsto \overline{\varphi}$. Next we want to prove, that this map truly is a homomorphism of R-modules. That is we consider any two multi-linear maps φ and ψ from $M_1 \times \cdots \times M_n$ to N. If now $a \in R$ is any scalar then from $\overline{a\varphi}\tau = a\varphi$ we get $\overline{a\varphi}(x_1 \otimes \ldots \otimes x_n) = (a\varphi)(x_1, \ldots, x_n) = a\varphi(x_1, \ldots, x_n) = a\overline{\varphi}(x_1 \otimes \ldots \otimes x_n)$ and hence $\overline{a\varphi} = a\overline{\varphi}$ as these elements generate $M_1 \times \cdots \times M_n$. Likewise $\overline{\varphi + \psi} = (\varphi + \psi)\tau$ implies $(\overline{\varphi + \psi})(x_1 \otimes \ldots \otimes x_n) = (\varphi + \psi)(x_1, \ldots, x_n) = \varphi(x_1, \ldots, x_n) + \psi(x_1, \ldots, x_n) = \overline{\varphi}(x_1 \otimes \ldots \otimes x_n) + \overline{\psi}(x_1 \otimes \ldots \otimes x_n)$ such that $\overline{\varphi + \psi} = \overline{\varphi} + \overline{\psi}$ again. So we have also proved the homomorphism property and it only remains to show the bijectivety: The injectivety is clear again, as $\overline{\varphi} = \overline{\psi}$ implies $\varphi = \overline{\varphi}\tau = \overline{\psi}\tau = \psi$. And given any homomorphism $\alpha : M_1 \times \cdots \times M_n \to N$ let us define $\varphi : X \to N$ by $\varphi(x_1, \ldots, x_n) := \alpha(x_1 \otimes \ldots \otimes x_n)$. Then it is clear, that $\varphi = \alpha\tau$ by construction and hence φ is R-multi-linear. But from this we also get $\alpha = \overline{\varphi}$ which in turn is the surjectivety of $\varphi \mapsto \overline{\varphi}$. □

Proof of (3.144):

(i) Let us abbreviate $M := M_1 \otimes \ldots \otimes M_n$ and $M_\sigma := M_{\sigma(1)} \otimes \ldots \otimes M_{\sigma(n)}$. It is clear that for any permutation $\sigma \in S_n$ the following map is (bijective and) R-multilinear

$$\lambda_\sigma \ : \ \bigoplus_{i=1}^{n} M_i \to \bigoplus_{i=1}^{n} M_{\sigma(i)} : (x_1, \ldots, x_n) \mapsto (x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$

Hence the composition $\tau\lambda_\sigma$ (where τ is the standard map, that turns tuples into tensors) which takes $(x_1, \ldots, x_n)$ to $x_{\sigma(1)} \otimes \ldots \otimes x_{\sigma(n)}$ is R-multilinear again. According to the universal property of tensor products (3.142) it therefore induces an R-linear map $\pi_\sigma := \overline{\tau\lambda_\sigma} : M \to M_\sigma$, by linear expansion of $x_1 \otimes \ldots \otimes x_n \mapsto x_{\sigma(1)} \otimes \ldots \otimes x_{\sigma(n)}$. It is clear that π_σ admits an inverse - namely $\pi_{\sigma^{-1}}$ and hence is is the R-module isomorphism that has been claimed

$$\pi_\sigma \ : \ M \ \xrightarrow{\sim} \ M_\sigma$$

(ii) In this prove let us abbreviate $M := M_1 \otimes \ldots \otimes M_n$ and $N(j) := M_{i(j,1)} \otimes \ldots M_{i(j,r(j))}$ for $j \in 1 \ldots s$. Then we need to show the isomorphy of $M \ \cong_{\mathsf{m}} \ N(1) \otimes \ldots \otimes N(s)$. We will prove this statement by induction on s, the case $s = 1$ having been proved in (i). In the case $s = 2$ we are given two sets $I' := I(1)$ and $I'' := I(2)$ such that $I = I' \cup I''$ and $I' \cap I'' = \emptyset$. Likewise let $M' := N(1)$ and $M'' := N(2)$. By renaming let us assume $I' = \{\, 1, \ldots, r-1 \,\}$ and $I'' = \{\, r, \ldots, n \,\}$ (note that the

order of the indexes does not matter, according to (i)). Then we will show the following isomorphy of R-modules

$$M \xrightarrow{\sim} M' \otimes M'' \,:\, x_1 \otimes \ldots \otimes x_n \mapsto (x_1 \otimes \ldots \otimes x_{r-1}) \otimes (x_r \otimes \ldots \otimes x_n)$$

To do this note that the map $\varphi : M_1 \times \cdots \times M_n \to M' \otimes M''$ given, by $\varphi(x_1, \ldots, x_n) := (x_1 \otimes \ldots \otimes x_{r-1}) \otimes (x_r \otimes \ldots \otimes x_n)$ is R-multi-linear. We will prove this for the first argument only, as the other arguments are completely analogous:

$$\begin{aligned}
\varphi(ax_1, x_2, \ldots, x_n) &= (ax_1) \otimes x_2 \otimes \ldots \otimes x_n \\
&= a(x_1 \otimes x_2 \otimes \ldots \otimes x_n) \\
&= a\varphi(x_1, x_2, \ldots, x_n) \\
\varphi(x_1 + x_1', x_2, \ldots, x_n) &= (x_1 + x_1') \otimes x_2 \otimes \ldots \otimes x_n \\
&= x_1 \otimes x_2 \otimes \ldots \otimes x_n + x_1' \otimes x_2 \otimes \ldots \otimes x_n \\
&= \varphi(x_1, x_2, \ldots, x_n) + \varphi(x_1', x_2, \ldots, x_n)
\end{aligned}$$

Therefore the universal property (3.142) yields an R-linear map $\Phi := \overline{\varphi} : M \to M' \otimes M''$ which is defined by linear expansion of $x_1 \otimes \ldots \otimes x_n \mapsto (x_1 \otimes \ldots \otimes x_{r-1}) \otimes (x_r \otimes \ldots \otimes x_n)$ so it only remains to show the bijectivity of this map. In order to do so, let us construct the inverse map, starting with $\psi : M' \times M'' \to M$ defined by linear expansion of

$$\psi \,:\, (x_1 \otimes \ldots \otimes x_{r-1}, x_r \otimes \ldots \otimes x_n) \mapsto x_1 \otimes \ldots \otimes x_n$$

which is clearly well-defined, as the tensor product identifies more elements, than the direct sum does. And it also is R-multi-linear, as it has been defined by linear expansion. Thus we again find an R-linear map $\Psi := \overline{\psi} : M' \otimes M'' \to M$ by linear expansion of $(x_1 \otimes \ldots \otimes x_{r-1}) \otimes (x_r \otimes \ldots \otimes x_n) \mapsto x_1 \otimes \ldots \otimes x_n$. It is obvious that Ψ is the inverse of Φ which makes Φ and isomorphism. For arbitrary $s \geq 2$ let us denote $I' := I(1)$ and $I'' := I(2) \cup \cdots \cup I(s)$. For ease of notation we again assume that $I' = \{1, \ldots, r-1\}$ such that $I'' = \{r, \ldots, n\}$ as well. In the case $s = 2$ we have just shown the isomorphy

$$M \xrightarrow{\sim} M' \otimes M'' \,:\, x_1 \otimes \ldots \otimes x_n \mapsto (x_1 \otimes \ldots \otimes x_{r-1}) \otimes (x_r \otimes \ldots \otimes x_n)$$

(note that this map and all the maps to follow are uniquely determined by their action on the pure tensor products and act by linear expansion on linear combinations of these). And by induction hypothesis we can rely on the isomorphy

$$\begin{aligned}
\bigotimes_{i=r}^{n} M_i &\xrightarrow{\sim} \bigotimes_{j=2}^{s} N(j) \\
x_r \otimes \ldots \otimes x_n &\mapsto \otimes_{j=2}^{s} \big(\otimes_{k=1}^{r(j)} x_{i(j,k)} \big)
\end{aligned}$$

So combining these two we have arrived at the following isomorphy

$$\begin{array}{rcl} M & \xrightarrow{\sim} & N(1) \otimes \left(\bigotimes_{j=2}^{s} N(j) \right) \\ x_1 \otimes \ldots \otimes x_n & \mapsto & (x_1 \otimes \ldots \otimes x_{r-1}) \otimes \left(\otimes_{j=2}^{s} \left(\otimes_{k=1}^{r(j)} x_{i(j,k)} \right) \right) \end{array}$$

But for any R-modules $N(1)$, $N(2)$ to $N(s)$ the case $s = 2$ has also proved the following isomorphy of R-modules

$$\begin{array}{rcl} \bigotimes_{j=1}^{n} N(j) & \xrightarrow{\sim} & N(1) \otimes \left(\bigotimes_{j=2}^{s} N(j) \right) \\ n_1 \otimes \ldots \otimes n_s & \mapsto & n_1 \otimes (n_2 \otimes \ldots \otimes n_s) \end{array}$$

So attaching the inverso of this isomorphism to the isomorphism we have constructed so far, we have finally arrived at the isomorhism, that has been given in the claim

$$\begin{array}{rcl} M & \xrightarrow{\sim} & \bigotimes_{j=1}^{s} N(j) \\ x_1 \otimes \ldots \otimes x_n & \mapsto & \otimes_{j=1}^{s} \left(\otimes_{k=1}^{r(j)} x_{i(j,k)} \right) \end{array}$$

(iii) Let us denote $A := A_1 \times \cdots \times A_n$ and $P := A_1 \otimes \ldots \otimes A_n$ (as an R-module). Let us also abbreviate $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n) \in A$. Then, for a fixed y, we now regard the map

$$\mu_y : A \to P : (x_1, \ldots, x_n) \mapsto (x_1 y_1) \otimes \ldots \otimes (x_n y_n)$$

Note that the multiplication $x_i y_i$ is that of the semi-algebra A_i. It is easy to see that this map is R-multi-linear - we will verify this for the first component A_i only (as the others are completely analogous):

$$\begin{array}{rcl} \mu_y(a x_1, x_2, \ldots, x_n) & = & (a x_1 y_1) \otimes (x_2 y_2) \otimes \ldots \otimes (x_n y_n) \\ & = & a (x_1 y_1) \otimes (x_2 y_2) \otimes \ldots \otimes (x_n y_n) \\ & = & a \mu_y(x_1, x_2, \ldots, x_n) \\ \mu_y(x_1 + x_1', x_2, \ldots, x_n) & = & ((x_1 + x_1') y_1) \otimes (x_2 y_2) \otimes \ldots \otimes (x_n y_n) \\ & = & (x_1 y_1) \otimes (x_2 y_2) \otimes \ldots \otimes (x_n y_n) \\ & & + (x_1' y_1) \otimes (x_2 y_2) \otimes \ldots \otimes (x_n y_n) \\ & = & \mu_y(x_1, x_2, \ldots, x_n) + \mu_y(x_1', x_2, \ldots, x_n) \end{array}$$

Therefore μ_y induces an R-linear map $\lambda_y := \overline{\mu_y} : P \to P$ again, by virtue of the universal property (3.142), by linear expansion of the the operation $x_1 \otimes x_2 \otimes \ldots \otimes x_n \mapsto (x_1 y_1) \otimes (x_2 y_2) \otimes \ldots \otimes (x_n y_n)$. If we are now given some $b_j \in R$ and $y(j) = (y_{j,1}, \ldots, y_{j,n}) \in A$ (where $j \in 1 \ldots \ell$) then

the linear combination of R-linear maps $b_1\lambda_{y(1)} + \ldots b_\ell\lambda_{y(\ell)}$ is given to be the following:

$$\sum_{i=1}^{k} a_i\, x_{i,1} \otimes \ldots \otimes x_{i,n} \;\mapsto\; \sum_{i=1}^{k}\sum_{j=1}^{\ell} a_i\, b_j\, (x_{i,1}y_{j,1}) \otimes \ldots \otimes (x_{i,n}y_{j,n})$$

So this is precisely the expression we have used to define the multiplication on P. And as the b_j and $y(j)$ have been arbitrary this means the expression is truly well-defined. And the properties of an R-algebra (like associativity, distributivity and compatibility with the scalar multiplication) are immediately clear by regarding this explicit definition.

□

Proof of (3.145):
Existence: Clearly the map $\alpha : A_1 \times \cdots \times A_n \to B$ defined by $\alpha(x_1, \ldots, x_n) := \alpha_1(x_1) \cdot \cdots \cdot \alpha_n(x_n)$ is R-multilinear. Hence by the universal property (3.142) of tensor products it gives rise to a well defined, R-module homomorphism $\overline{\alpha}$ which is defined by linear expansion of

$$\overline{\alpha} \;:\; A_1 \otimes \ldots \otimes A_n \to B \;:\; x_1 \otimes \ldots \otimes x_n \mapsto \alpha_1(x_1) \cdot \cdots \cdot \alpha_n(x_n)$$

It remains to prove that $\overline{\alpha}$ truly is multiplicative. But of course it suffices to verify this for pure tensors, as these generate $A_1 \otimes \ldots \otimes A_n$ already. So compute

$$\begin{aligned}
\overline{\alpha}\left(\left(\bigotimes_{i=1}^{n} x_i\right) \cdot \left(\bigotimes_{i=1}^{n} y_i\right)\right) &= \overline{\alpha}\left(\bigotimes_{i=1}^{n}(x_i y_i)\right) \\
&= \prod_{i=1}^{n} \alpha_i(x_i y_i) \;=\; \prod_{i=1}^{n} \alpha_i(x_i)\alpha_i(y_i) \\
&= \left(\prod_{i=1}^{n} \alpha_i(x_i)\right)\left(\prod_{i=1}^{n} \alpha_i(y_i)\right) \\
&= \overline{\alpha}\left(\bigotimes_{i=1}^{n} x_i\right) \cdot \overline{\alpha}\left(\bigotimes_{i=1}^{n} y_i\right)
\end{aligned}$$

Thereby we used the fact that all the $\alpha_i(x_i)$ and $\alpha_j(y_j)$ are mutually commutative, as the images of the α_i is contained in the center of B, by asumption. It remains to verify the *Uniqueness:* by assumption $\overline{\alpha}$ had to satisfy $\overline{\alpha}(\overline{x}_j) = \alpha_j(x_j)$. But it is clear that $\prod_i \overline{x}_i = \otimes_i x_i$ so again we may compute

$$\overline{\alpha}\left(\bigotimes_{i=1}^{n} x_i\right) \;=\; \overline{\alpha}\left(\prod_{i=1}^{n} \overline{x}_i\right) \;=\; \prod_{i=1}^{n} \overline{\alpha}\,(\overline{x}_i) \;=\; \prod_{i=1}^{n} \alpha_i(x_i)$$

That is: the restrictions we imposed on $\overline{\alpha}$ uniquely determine the action of $\overline{\alpha}$ on the pure tensors $x_1 \otimes \ldots \otimes x_n$. But as these generate $A_1 \otimes \ldots \otimes A_n$ and $\overline{\alpha}$ is R-linear, this determines $\overline{\alpha}$ for all tensor elements. □

Proof of (3.146):

(i) Since M is an R-module and R is a *commutative* ring the map $R \times M \to M : (a, x) \mapsto ax$ is bilinear. So by the universal property of tensor products (3.142) we get a well-defined R-linear map $R \otimes M \to M$ by linear expansion of $a \otimes x \mapsto ax$. This clearly is surjective, as $1 \otimes x \mapsto x$ for

any $x \in M$ and if $ax = by$, then $a \otimes x = a(1 \otimes x) = 1 \otimes ax = 1 \otimes by = b(1 \otimes y) = b \otimes y$ which also is the injectivety of this map.

(ii) According to (3.40.(vi)) $M/\mathfrak{a}M$ is an $(R/\mathfrak{a})$-module under the scalar multiplication $(b + \mathfrak{a})(x + \mathfrak{a}M) := bx + \mathfrak{a}M$. Hence the map of the scalar multiplication is well-defined and R-bilinear

$$\varphi \ : \ {}^{R}\Big/_{\mathfrak{a}} \times M \to {}^{M}\Big/_{\mathfrak{a}M} \ : \ (b + \mathfrak{a}, x) \mapsto bx + \mathfrak{a}M$$

Hence (3.142) tells us that there is an R-linear map $\Phi := \overline{\varphi}$ again, which is given by linear expansion of

$$\Phi \ : \ {}^{R}\Big/_{\mathfrak{a}} \otimes M \to {}^{M}\Big/_{\mathfrak{a}M} \ : \ (b + \mathfrak{a}) \otimes x \mapsto bx + \mathfrak{a}M$$

This map clearly is surjective, as for any $x \in M$ we get $(1 + \mathfrak{a}) \otimes x \mapsto x + \mathfrak{a}M$. And to prove the injectivety we will show $\mathrm{kn}(\Phi) = 0$. So consider some element that is mapped to 0 under Φ:

$$\sum_{k=1}^{m} f_k(b_k + \mathfrak{a}) \otimes x_k \ \mapsto \ \sum_{k=1}^{m} f_k b_k x_k + \mathfrak{a}M \ = \ 0 + \mathfrak{a}M$$

which is nothing but $\sum_k f_k b_k x_k \in \mathfrak{a}M$. That is there are some $a_i \in \mathfrak{a}$ and $u_i \in M$ (where $i \in 1 \dots n$) such that $\sum_k f_k b_k x_k = \sum_i a_i u_i$. And using this we can compute

$$\begin{aligned}
\sum_{k=1}^{m} f_k(b_k + \mathfrak{a}) \otimes x_k &= \sum_{k=1}^{m} (1 + \mathfrak{a}) \otimes (f_k b_k x_k) \\
&= (1 + \mathfrak{a}) \otimes \left(\sum_{k=1}^{m} f_k b_k x_k \right) \\
&= (1 + \mathfrak{a}) \otimes \left(\sum_{i=1}^{n} a_i u_i \right) \\
&= \sum_{i=1}^{n} (1 + \mathfrak{a}) \otimes (a_i u_i) \\
&= \sum_{i=1}^{n} (a_i + \mathfrak{a}) \otimes u_i \ = \ 0
\end{aligned}$$

the latter, since $a_i + \mathfrak{a} = 0 + \mathfrak{a}$ annihilating every single summand. Thus we have $\mathrm{kn}(\Phi) = 0$ which is the injectivity of Φ, such that we truly have our isomorphism.

(iii) By construction of the tensor product an element $t \in (R/\mathfrak{a}) \otimes (R/\mathfrak{b})$ is of the form $t = \sum_i a_i(r_i + \mathfrak{a}) \otimes (s_i + \mathfrak{b})$. But it is clear that

$$\sum_{i=1}^{m} a_i(r_i + \mathfrak{a}) \otimes (s_i + \mathfrak{b}) \ = \ (1 + \mathfrak{a}) \otimes \left(\sum_{i=1}^{m} a_i r_i s_i + \mathfrak{b} \right)$$

Hence we have proved, that any element t can be written in the form $(1 + \mathfrak{a}) \otimes (r + \mathfrak{b})$ for some $r \in R$. Now consider the following map

$${}^{R}\Big/_{\mathfrak{a}} \times {}^{R}\Big/_{\mathfrak{b}} \to {}^{R}\Big/_{\mathfrak{a}+\mathfrak{b}} \ : \ (r + \mathfrak{a}, s + \mathfrak{b}) \mapsto rs + (\mathfrak{a} + \mathfrak{b})$$

This is well defined, since $\mathfrak{a}$ and $\mathfrak{b} \subseteq \mathfrak{a} + \mathfrak{b}$ and bilinear, since R is commutative. By the universal

property of the tensor product we find a well-defined, R-linear map by expansion of

$$R\big/_{\mathfrak{a}} \otimes R\big/_{\mathfrak{b}} \to R\big/_{\mathfrak{a}+\mathfrak{b}} \;:\; (r+\mathfrak{a}) \otimes (s+\mathfrak{b}) \mapsto rs + (\mathfrak{a}+\mathfrak{b})$$

Clearly this map is surjective, as for any $s \in R$ we find $(1+\mathfrak{a}) \otimes (s+\mathfrak{b}) \mapsto s + (\mathfrak{a}+\mathfrak{b})$. But it also is injective: To prove this we will show that is has zero-kernel. That is we regard any r, $s \in R$ such that $rs + (\mathfrak{a}+\mathfrak{b}) = 0$. But this means $rs \in \mathfrak{a}+\mathfrak{b}$ or in other words $rs = a+b$ for some $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$. This now enables us compute $(r+\mathfrak{a}) \otimes (s+\mathfrak{b}) = (1+\mathfrak{a}) \otimes (rs+\mathfrak{b}) = (1+\mathfrak{a}) \otimes (a+b+\mathfrak{b}) = (1+\mathfrak{a}) \otimes (a+\mathfrak{b}) = (a+\mathfrak{a}) \otimes (1+\mathfrak{b}) = (0+\mathfrak{a}) \otimes (1+\mathfrak{b}) = 0$.

(iv) The strategy of this proof is very similar to the one in (ii). We take the scalar multiplication of the $U^{-1}R$-module $U^{-1}M$ again

$$\varphi \;:\; U^{-1}R \times M \to U^{-1}M \;:\; \left(\frac{b}{u}, x\right) \mapsto \frac{bx}{u}$$

which is R-bilinear, since it is a scalar multiplication. So this induces an R-linear $\Phi := \overline{\varphi}$ again, which is given by linear expansion of

$$\Phi \;:\; U^{-1}R \otimes M \to U^{-1}M \;:\; \left(\frac{b}{u}\right) \otimes x \mapsto \frac{bx}{u}$$

As before the surjectivity is clear, since $(1/u) \otimes x \mapsto x/u$ for any $x \in M$ and $u \in U$. And to prove the injectivety we will show $\mathrm{kn}(\Phi) = 0$. So consider some element that is mapped to $0 \in U^{-1}M$ under Φ, then all that remains to prove that this element is $0 \in U^{-1}R \otimes M$ already:

$$\sum_{k=1}^{m} a_k \, \frac{b_k}{u_k} \otimes x_k \;\mapsto\; \sum_{k=1}^{m} \frac{a_k b_k x_k}{u_k} \;=\; \frac{0}{1}$$

Let us denote $u := u_1 \cdot \cdots \cdot u_m$ and $\widehat{u}_k := u/u_k \in U$ then the latter means there is some $v \in U$ such that $v \sum_k a_k b_k \widehat{u}_k x_k = 0$. And using this we can compute

$$\begin{aligned}
\sum_{k=1}^{m} a_k \, \frac{b_k}{u_k} \otimes x_k &= \sum_{k=1}^{m} \frac{a_k b_k \widehat{u}_k v}{uv} \otimes x_k \\
&= \frac{1}{uv} \otimes \left(\sum_{k=1}^{m} a_k b_k \widehat{u}_k v x_k \right) \\
&= \frac{1}{uv} \otimes 0 \;=\; 0
\end{aligned}$$

(v) Let us denote the map given in the claim, by $\Phi : (y_i) \mapsto \sum_i m_i \otimes y_i$. This is well-defined, since $y_i = 0$ for all but finitely many $i \in I$ such that in truth the sum is finitely only. Also it is R-linear, which is obvious from the construction. We will now prove its bijectivity by constructing its inverse map $\Lambda = \Phi^{-1}$. To do this let us denote the coordinate function of m_j by $\mu_j : M \to R : \sum_i a_i m_i \mapsto a_j$. This construction is possible, since $\{ m_i \mid i \in I \}$ i a basis and hence the coefficient a_j of $x = \sum_i a_i m_i$ is uniquely determined. Also μ_j is R-linear and we get $\mu_j(m_i) = \delta_{i,j}$ for any i,

$j \in I$ and $x = \sum_i \mu_i(x) m_i$ for any $x \in M$. Therefore the map

$$\lambda \;:\; M \times N \to N^{\oplus I} \;:\; (x,y) \mapsto \big(\mu_i(x)y\big)_{i\in I}$$

is R-bilinear (which is obvious from the construction) and therefore induces an R-linear map $\Lambda := \overline{\lambda}$ by linear expansion of

$$\Lambda \;:\; M \otimes N \to N^{\oplus I} \;:\; x \otimes y \mapsto \big(\mu_i(x)y\big)_{i\in I}$$

Using this map we will now prove that truly $\Lambda = \Phi^{-1}$ is the inverse of Φ, such that Φ truly is an isomorphism. It suffices to check this on the generating set of pure tensors $x \otimes y$, however:

$$\begin{aligned}
\Phi\Lambda(x\otimes y) &= \Phi\big(\mu_i y\big) \\
&= \sum_{i\in I} m_i \otimes (\mu_i(x)y) \\
&= \sum_{i\in I} (\mu_i(x) m_i) \otimes \mu_i(x) y \\
&= \left(\sum_{i\in I} \mu_i(x) m_i\right) \otimes \mu_i(x) y \;=\; x \otimes y \\
\Lambda\Phi(y_i) &= \Lambda\left(\sum_{j\in I} m_j \otimes y_j\right) \\
&= \sum_{j\in I} \Lambda(m_j \otimes y_j) \\
&= \sum_{j\in I} \big(\mu_i(m_j) y_j\big)_{i\in I} \\
&= \sum_{j\in I} \big(\delta_{i,j} y_j\big)_{i\in I} \;=\; (y_i)
\end{aligned}$$

(vi) Since $\big\{\, n_j \mid j \in J \,\big\}$ is an R-basis of N we clearly have the isomorphy $R^{\oplus J} \xrightarrow{\sim} N : (b_j) \mapsto \sum_j b_j n_j$. Also there is a natural isomorphy given by $R^{\oplus(I\times J)} \xrightarrow{\sim} (R^{\oplus I})^{\oplus J} : (a_{i,j}) \mapsto ((a_{i,j})_j)_i$. Inserting the first in the latter we arrive at the following isomorphy of R-modules

$$R^{\oplus(I\times J)} \;\xrightarrow{\sim}\; N^{\oplus I} \;:\; (a_{i,j}) \;\mapsto\; \left(\sum_{j\in J} a_{i,j} n_j\right)_{i\in I}$$

But according to (iv) we also have the isomorphy $N^{\oplus I} \xrightarrow{\sim} M \otimes N$ given by $(y_i) \mapsto \sum_i m_i \otimes y_i$. If we append this isomorphism to the one above we finally arrive at the following isomorphy

$$\Phi \;:\; R^{\oplus(I\times J)} \;\xrightarrow{\sim}\; M \otimes N \;:\; (a_{i,j}) \;\mapsto\; \sum_{i\in I} m_i \otimes \left(\sum_{j\in J} a_{i,j} n_j\right)$$

Using the linearity of the tensor product in the second argument we finally find that this isomorphism truly maps onto an R-linear combination of the $m_i \otimes n_j$

$$\Phi(a_{i,j}) \;=\; \sum_{i\in I}\sum_{j\in J} a_{i,j}\, m_i \otimes n_j \;=\; \sum_{(i,j)\in I\times J} a_{i,j}\, m_i \otimes n_j$$

So this map transfers the standard Euclidean basis $\left\{ e_{(i,j)} \mid i \in I, j \in J \right\}$ of $R^{\oplus(I\times J)}$ onto the pure tensors $\left\{ m_i \otimes y_j \mid i \in I, j \in J \right\}$. And as it is an isomorphism this truly proves, that this set is an R-basis of $M \otimes N$.

(vii) This proof follows the same general ideas as the proof of (iv): Let $M := \oplus_i M_i$ and $N := \oplus_j N_j$ be the direct sums of the R-modules M_i and N_j respectively. We consider the $M_i \subseteq M$ and $N_j \subseteq N$ to be sub-modules of these, canonically. For any fixed $i \in I$ and $j \in J$ we then regard the canonical morphism

$$\iota_{i,j} \ : \ M_i \times N_j \to M \otimes N \ : \ (x_i, y_j) \mapsto x_i \otimes y_j$$

As the tensor product $x_i \otimes y_j$ is bilinear, so is $\iota_{i,j}$ such that it induces an R-linear map $\varphi_{i,j} := \bar{\iota}_{i,j}$, by linear expansion of

$$\varphi_{i,j} \ : \ M_i \otimes N_j \to M \otimes N \ : \ x_i \otimes y_j \mapsto x_i \otimes y_j$$

We now build up the sum of all these R-module homomorphisms, that is we compose $\oplus_{(i,j)}\varphi_{i,j} : \oplus_{i,j}(M_i \otimes N_j) \to (M \otimes N)^{\oplus(I\times J)}$ with the map $\Sigma : (M \otimes N)^{\oplus(I\times J)} \to M \otimes N : (f_{i,j}) \mapsto \sum_i \sum_j f_{i,j}$. Thereby Σ is well-defined as we have $f_{i,j} \neq 0$ for only finitely many $(i,j) \in I \times J$. And it is R-linear by construction. Altogether we obtain an R-linear map $\Phi := \Sigma \oplus_{(i,j)} \varphi_{i,j}$ which is thereby defined by linear expansion of

$$\Phi \ : \ \bigoplus_{(i,j)\in I\times J} (M_i \otimes N_j) \to M \otimes N \ : \ (x_i \otimes y_j) \mapsto \sum_{i\in I}\sum_{j\in J} x_i \otimes y_i$$

We will now prove that Φ is bijective, by constructing its inverse map. To do this note that any $x \in M$ has a unique decomposition into $x = \sum_i x_i$ such that $x_i \in M_i$ for all $i \in I$. Likewise $y \in N$ can be decomposed into $y = \sum_j y_j$ with $y_j \in N_j$.Therefore the following map (the canonocal projection) is well-defined

$$\pi_{i,j} \ : \ M \times N \to M_i \otimes N_j \ : \ (x, y) \mapsto x_i \otimes y_j$$

This map clearly is R-bilinear and hence induces an R-linear map by linear expansion of

$$\psi_{i,j} \ : \ M \otimes N \to M_i \otimes N_j \ : \ x \otimes y \mapsto x_i \otimes y_j$$

Let us join these R-module homomorphisms into the direct sum of the $M_i \otimes N_j$ defining the following R-linear map by linear expansion of

$$\Psi \ : \ M \otimes N \to \bigoplus_{(i,j)\in I\times J} (M_i \otimes N_j) \ : \ x \otimes y \mapsto (x_i \otimes y_i)$$

That is Ψ is precisely the map of which we claim that it is an isomorphism. But we will now prove that Φ already is the inverse of this map $\Psi = \Phi^{-1}$ such that Φ truly is an isomorphism. It suffices to check this on the generating set of pure tensors $x \otimes y$, however:

$$\Phi\Psi(x \otimes y) \quad = \quad \Phi\big(x_i \otimes y_j\big)$$

$$
\begin{aligned}
&= \sum_{i\in I}\sum_{j\in J} x_i \otimes y_j \\
&= \sum_{i\in I} x_i \otimes \left(\sum_{j\in J} y_j\right) \\
&= \sum_{i\in I} x_i \otimes y \\
&= \left(\sum_{i\in I} x_i\right) \otimes y \;=\; x \otimes y \\
\Psi\Phi(x_i \otimes y_j) &= \Psi\left(\sum_{i\in I}\sum_{j\in I} x_i \otimes y_j\right) \\
&= \Psi(\dots \text{see above} \dots) \\
&= \Psi(x \otimes y) \;=\; (x_i \otimes y_j)
\end{aligned}
$$

(viii) For ease of notation let us denote $C := A \times C$ and let us denote the map that is claimed to be an isomorphism by Φ. Note that this is truly well defined, as for all but finitely many $(\alpha, \beta) \in C$ we have $f[\alpha, \beta] = 0$ and hence the sum is finite only, in truth

$$
\begin{aligned}
\Phi \;:\; R\left[x \mid C\right] &\to R\left[s \mid A\right] \otimes R\left[t \mid B\right] \\
\sum_{(\alpha,\beta)\in C} f\left[\alpha,\beta\right]\, x^{(\alpha,\beta)} &\mapsto \sum_{(\alpha,\beta)\in C} f\left[\alpha,\beta\right]\, s^{\alpha} \otimes t^{\beta}
\end{aligned}
$$

It also is clear, that Φ is R-linear, by definition of the addition and scalar multiplication in the polynomial ring $R[x \mid C]$. We will now prove that it even is an R-algebra-homomorphism: it is clear that $\Phi(1) = 1$ and we also get

$$
\begin{aligned}
\Phi\big(x^{(\alpha,\beta)} x^{(\gamma,\delta)}\big) &= \Phi\big(x^{(\alpha+\gamma,\beta+\delta)}\big) \;=\; s^{\alpha+\gamma} t^{\beta+\delta} \\
&= \big(s^{\alpha} t^{\beta}\big)\big(s^{\gamma} t^{\delta}\big) \;=\; \Phi\big(x^{(\alpha,\beta)}\big)\, \Phi\big(x^{(\gamma,\delta)}\big)
\end{aligned}
$$

Due to the R-linearity this expands to $\Phi(fg) = \Phi(f)\Phi(g)$ for any two polynomials $f, g \in R[x \mid C]$. So it only remains to show that Φ truly is an R-alebra isomorphism, so we will prove its bijectivity by constructiong its inverse map Ψ again. Let us start with

$$
\begin{aligned}
R\left[s \mid A\right] \times R\left[t \mid B\right] &\to R\left[x \mid C\right] \\
\left(\sum_{\alpha\in A} f[\alpha]\, s^{\alpha}, \sum_{\beta\in B} g[\alpha]\, t^{\beta}\right) &\mapsto \sum_{(\alpha,\beta)\in C} f[\alpha] g[\beta]\, x^{(\alpha,\beta)}
\end{aligned}
$$

This map clearly is R-bilinear and hence induces an R-linear map by virtue of the universal property (3.142) given by linear expansion of

$$
\begin{aligned}
R\left[s \mid A\right] \otimes R\left[t \mid B\right] &\to R\left[x \mid C\right] \\
\left(\sum_{\alpha\in A} f[\alpha]\, s^{\alpha}\right) \otimes \left(\sum_{\beta\in B} g[\alpha]\, t^{\beta}\right) &\mapsto \sum_{(\alpha,\beta)\in C} f[\alpha] g[\beta]\, x^{(\alpha,\beta)}
\end{aligned}
$$

As always it remains to show $\Phi = \Psi^{-1}$ on the generating sets (even an R-basis) $x^{(\alpha,\beta)}$ and $s^{\alpha} \otimes t^{\beta}$

respectively. So let us compute

$$\Psi\Phi\big(x^{(\alpha,\beta)}\big) \;=\; \Psi\big(s^\alpha \otimes t^\beta\big) \;=\; x^{(\alpha,\beta)}$$

$$\Phi\Psi\big(s^\alpha \otimes t^\beta\big) \;=\; \Phi\big(x^{(\alpha,\beta)}\big) \;=\; s^\alpha \otimes t^\beta$$

□

Proof of (3.149):
The claims (i) and (ii) are obvious from the explicit definiton of the tensor product $\varphi_1 \otimes \ldots \otimes \varphi_n$, as:

$$\begin{aligned}
&\left(\bigotimes_{i=1}^n \psi_i\right)\left(\bigotimes_{i=1}^n \varphi_i\right)\left(\sum_{k=1}^m a_k\, x_{1,k} \otimes \ldots \otimes x_{n,k}\right)\\
=\;&\left(\bigotimes_{i=1}^n \psi_i\right)\left(\sum_{k=1}^m a_k\, \varphi_1(x_{1,k}) \otimes \ldots \varphi_n(\otimes x_{n,k})\right)\\
=\;&\sum_{k=1}^m a_k\, \psi_1\varphi_1(x_{1,k}) \otimes \ldots \psi_n\varphi_n(\otimes x_{n,k})\\
=\;&\bigotimes_{i=1}^n(\psi_i\varphi_i)\left(\sum_{k=1}^m a_k\, x_{1,k} \otimes \ldots \otimes x_{n,k}\right)
\end{aligned}$$

So in case all φ_i are bijective we find inverse maps $\varphi_i^{-1} : M_i \to L_i$ such that $\varphi_i\varphi_i^{-1} = \mathbb{1}_i$ and $\varphi_i^{-1}\varphi_i = \mathbb{1}_i$. And due to (i) and (ii) this readily implies

$$\left(\bigotimes_{i=1}^n \varphi_i^{-1}\right)\left(\bigotimes_{i=1}^n \varphi_i\right) \;=\; \bigotimes_{i=1}^n(\varphi_i^{-1}\varphi_i) \;=\; \bigotimes_{i=1}^n \mathbb{1}_i \;=\; \mathbb{1}_{L_1\otimes\ldots\otimes L_n}$$

$$\left(\bigotimes_{i=1}^n \varphi_i\right)\left(\bigotimes_{i=1}^n \varphi_i^{-1}\right) \;=\; \bigotimes_{i=1}^n(\varphi_i\varphi_i^{-1}) \;=\; \bigotimes_{i=1}^n \mathbb{1}_i \;=\; \mathbb{1}_{M_1\otimes\ldots\otimes M_n}$$

Such that $\varphi_1^{-1} \otimes \ldots \otimes \varphi_n^{-1}$ is the inverse map of $\varphi_1 \otimes \ldots \otimes \varphi_n$ and in particular this is the bijectivity of $\varphi_1 \otimes \ldots \otimes \varphi_n$ again. Also if all the φ_i are surjective then for any $y_i \in M_i$ there is some $x_i \in L_i$ such that $\varphi_i(x_i) = y_i$. That is we find that $x_1 \otimes \ldots \otimes x_n$ is mapped to $y_1 \otimes \ldots \otimes y_n$ under $\varphi_1 \otimes \ldots \otimes \varphi_n$. But as the pure tensors $y_1 \otimes \ldots \otimes y_n$ generate $M_1 \otimes \ldots \otimes M_n$ and the y_i have been arbitrary that already is the surjectivity of $\varphi_1 \otimes \ldots \otimes \varphi_n$ again. That is we have proved the first two statements of (iii) as well. The injectivity part of (iii) (where R is a field) is a direct consequence of (iv) however, as in case of a vectorspace M_i *all* sub-modules are complemented. That is since R is a field property (b) of (iv) is granted automatically, so (a) of (iv) already states the injectivity of $\varphi_1 \otimes \ldots \otimes \varphi_n$. It remains to prove (iv):

Due to assumption (2) we have $M_i = \mathrm{im}(\varphi_i) \oplus P_i$ that is any $z_i \in M_i$ can be written in a unique way as $z_i = y_i + p_i$ with $y_i \in \mathrm{im}(\varphi_i)$ and $p_i \in P_i$. And hence we can define R-module homomorphism $\pi_i : M_i \to \mathrm{im}(\varphi_i)$, by letting $\pi_i(z_i) := y_i$ for this y_i. But as φ_i is injective due to assumption (1) and $y_i \in \mathrm{im}(\varphi_i)$ there is a uniquely determined $x_i \in L_i$ such that $\varphi_i(x) = y_i$. That is may even define $\psi_i : M_i \to L_i$ by letting $\psi_i(z_i) := x_i$ for this x_i. By construction it is clear, that $\psi_i\varphi_i(x_i) = \psi_i(y_i) = x_i$

and therefore we get

$$\left(\bigotimes_{i=1}^{n}\psi_i\right)\left(\bigotimes_{i=1}^{n}\varphi_i\right) \;=\; \bigotimes_{i=1}^{n}(\psi_i\varphi_i) \;=\; \bigotimes_{i=1}^{n}\mathbb{1}_i \;=\; \mathbb{1}_{L_1\otimes\ldots\otimes L_n}$$

again which implies the injectivity of $\varphi_1\otimes\ldots\otimes\varphi_n$. Let us now abbreviate $L := \otimes_i L_i$, $M := \otimes_i M_i$ and $\varphi := \otimes_i\varphi_i : L \hookrightarrow M$, $\psi := \otimes_i\psi_i : M \twoheadrightarrow L$. Then we have seen $\psi\varphi = \mathbb{1}_L$ and we pick up $P := \mathrm{kn}(\psi)$. We will first prove that $M = \mathrm{im}(\varphi) + P$, that is we are given some $z \in M$ and need to find $y \in \mathrm{im}(\varphi)$ and $p \in P$ such that $z = y + p$. This can be done by taking $y := \varphi\psi(z) \in \mathrm{im}(\varphi)$ and $p := z - y$. It only remains to show $p \in P = \mathrm{kn}(\psi)$. But this is easy, since

$$\psi(p) = \psi(z-y) = \psi(z) - \psi(y) = \psi(z) - \psi\varphi\psi(z) = \psi(z) - \mathbb{1}_L\psi(z) = 0$$

And in order to prove $\mathrm{im}(\varphi)\cap P = 0$ we consider some $y \in \mathrm{im}(\varphi)\cap P$ that is $\psi(y) = 0$ and $y = \varphi(x)$ for some $x \in L$. And thereby $0 = \psi(y) = \psi\varphi(x) = x$ such that $y = \varphi(0) = 0$. Altogether we have $M = \mathrm{im}(\varphi)\oplus P$, as claimed. □

Proof of (3.151):

(ii) Let us abbreviate the S-modules $P := U^{-1}M$ and $Q := U^{-1}U$. Recall the construction of the tensor product $P\otimes_S Q$ to be the residue module

$$P\otimes_S Q \;=\; S^{\oplus(P\times Q)}\Big/T_S$$

If we denote the canonical basis of $S^{\oplus(P\times Q)}$ by $\{\,f(p,q) \mid p\in P, q\in Q\,\}$ then the sub-module T_S is the sub-module generated by elements of the form $f(p,q)+f(p',q)-f(p+p',q)$ and $f(p,q)+f(p,q')-f(p',q+q')$ but also by $sf(p,q)-f(sp,q)$ and $sf(p,q)-f(p,sq)$ where p, $p'\in P$, q, $q'\in Q$ and $s\in S$.

If we regard P and Q as R-modules P_R and Q_R respectively, then we have $P_R = P$ and $Q_R = Q$ as sets. Therefore the tensor product $P_R\otimes_R Q_R$ is the residue module

$$P_R\otimes_R Q_R \;=\; R^{\oplus(P\times Q)}\Big/T_R$$

We denote the canonical basis of $R^{\oplus(P\times Q)}$ by $\{\,e(p,q) \mid p\in P, q\in Q\,\}$ an T_R is the sub-module generated by the analogous elements, as above - just replace f by e and s by $a\in R$. Therefore we may define

$$\beta \;:\; R^{\oplus(P\times Q)} \;\to\; S^{\oplus(P\times Q)} \;:\; \sum_{k=1}^{m} a_k\, e(p_k,q_k) \;\mapsto\; \sum_{k=1}^{m} a_k\, f(p_k,q_k)$$

By definition β is injective and κ-linear [that is $\beta(ax) = \kappa(a)\beta(x)$]. However β need not be surjective, but it comes close: If we define $u := u_1\ldots u_m \in U$ and $\widehat{u}_k := u/u_k \in U$ then we find

$$\begin{aligned}\sum_{k=1}^{m}\frac{a_k}{u_k}f(p_k,q_k) \;&=\; \frac{1}{u}\sum_{k=1}^{m}\frac{\widehat{u}_k a_k}{1}f(p_k,q_k)\\ &=\; \frac{1}{u}\beta\left(\sum_{k=1}^{m}\widehat{u}_k a_k\, e(p_k,q_k)\right)\end{aligned}$$

As the scalar multiplication on P_R [that is P regarded as an R-module] is defined by $ap = (a/1)p$ we find the following identity

$$\beta\big(ae(p,q) - e(ap,q)\big) \;=\; \frac{a}{1}f(p,q) - f\left(\frac{a}{1}p,q\right) \;\in\; T_S$$

as we may take $s = a/1 \in S$. Likewise $\beta(ae(p,q) - e(p,aq)) \in T_S$ is plain to see. Altogether we find $\beta(T_R) \subseteq T_S$ from the identities

$$\begin{aligned}
\beta\big(e(p,q) + e(p',q) - e(p+p',q)\big) &= f(p,q) + f(p',q) - f(p+p',q)\\
\beta\big(e(p,q) + e(p,q') - e(p,q+q')\big) &= f(p,q) + f(p,q') - f(p,q+q')\\
\beta\big(ae(p,q) - e(ap,q)\big) &= \frac{a}{1}f(p,q) - f\left(\frac{a}{1}p,q\right)\\
\beta\big(ae(p,q) - e(p,aq)\big) &= \frac{a}{1}f(p,q) - f\left(p,\frac{a}{1}q\right)
\end{aligned}$$

Let us denote $1/U := \{\, 1/u \mid u \in U \,\} \subseteq S$ then conversely we find that $sf(p,q) - f(sp,q)$ is contained in $(1/U)\beta(T_R)$. To do this let $s = a/u \in S$ and $p' := sp \in P$, then $(u/1)p' = (a/1)p$ such that

$$\begin{aligned}
& sf(p,q) - f(sp,q)\\
=\;& \frac{a}{u}f(p,q) - f(p',q)\\
=\;& \frac{1}{u}\left(\frac{a}{1}f(p,q) - \frac{u}{1}f(p',q)\right)\\
=\;& \frac{1}{u}\left(\frac{a}{1}f(p,q) - f\left(\frac{a}{1}p,q\right) + f\left(\frac{u}{1}p',q\right) - \frac{u}{1}f(p',q)\right)\\
=\;& \frac{1}{u}\left(\beta\big(ae(p,q) - e(ap,q)\big) - \beta\big(ue(p',q) - e(up',q)\big)\right)
\end{aligned}$$

Likewise $sf(p,q) - f(p,q) \in (1/U)\beta(T_R)$ and altogether this implies the inclusion $T_S \subseteq (1/U)\beta(T_R)$. But as we also have $\beta(T_R) \subseteq T_S$ and T_S is an S-sub-module we find

$$T_S \;\subseteq\; \frac{1}{U}\beta(T_R) \;\subseteq\; \frac{1}{U}T_S \;\subseteq\; T_S \quad\Longrightarrow\quad T_S \;=\; \frac{1}{U}\beta(T_R)$$

As a final preparation we need the following map Φ_s (for any fixed $s \in S$) that is defined using the basis $e(p,q)$ again

$$\Phi_s \;:\; R^{\oplus(P\times Q)} \;\to\; R^{\oplus(P\times Q)} \;:\; \sum_{k=1}^{m} a_k\, e(p_k,q_k) \;\mapsto\; \sum_{k=1}^{m} a_k\, e(sp_k,q_k)$$

By definition it is clear that Φ_s is R-linear and for any $u \in U$ we have $\Phi_{(1/u)}\Phi_u = \mathbb{1}$ such that Φ_u is an automorphism. But for any $s \in S$ we also have $\Phi_s(T_R) \subseteq T_R$. This is due to $s(p+p') = sp + sp'$ and $sap = asp$ (as S is commutative). Therefore we get

$$\begin{aligned}
& \Phi_s\big(e(p,q) + e(p',q) - e(p+p',q)\big)\\
=\;& e(sp,q) + e(sp',q) - e(sp+sp',q)\\
& \Phi_s\big(e(p,q) + e(p,q') - e(p,q+q')\big)\\
=\;& e(sp,q) + e(sp,q') - e(sp,q+q')
\end{aligned}$$

and

$$\begin{aligned}\Phi_s\big(ae(p,q)-e(ap,q)\big) &= ae(sp,q)-e(asp,q)\\ \Phi_s\big(ae(p,q)-e(p,aq)\big) &= ae(sp,q)-e(sp,aq)\end{aligned}$$

which are all contained in T_R again. As T_R is generated by these elements and Φ_s is R-linear this truly means $\Phi_s(T_R) \subseteq T_R$. Let us now regard $\overline{\beta} := \varrho\beta$, that is $\overline{\beta}$ is the κ-linear map that is defined by $\overline{\beta}(x) = \beta(x) + T_S$ and hence is of the form

$$\overline{\beta} \;:\; R^{\oplus(P\times Q)} \;\to\; S^{\oplus(P\times Q)} \Big/ T_S \;=\; P \otimes_S Q$$

Note that in particular $\overline{\beta}(e(p,q)) = f(p,q) + T_S = p \otimes_S q$. Clearly $\overline{\beta}$ is surjective, as β came close to being surjective, such that

$$\sum_{k=1}^{m} \frac{a_k}{u_k}\, p_k \otimes_s q_k \;=\; \overline{\beta}\left(\sum_{k=1}^{m} \widehat{u}_k a_k e\left(\frac{1}{u}p_k, q_k\right)\right)$$

Also $\overline{\beta}(T_R) = \varrho\beta(T_R) \subseteq \varrho(T_S) = 0$ such that $T_R \subseteq \mathrm{kn}(\overline{\beta})$. Conversely if $x \in \mathrm{kn}(\overline{\beta})$ then $\beta(x) + T_S = \overline{\beta}(x) = 0$ which means $\beta(x) \in T_S = (1/U)\beta(T_R)$. That is $\beta(ux) = u\beta(x) \in \beta(T_R)$ for some $u \in U$. Hence $ux \in \beta^{-1}(\beta(T_R))$ and as β is injective this means $ux \in T_R$. Pick up a basis representation of x, that is $x = \sum_k a_k\, e(p_k, q_k)$, then

$$\begin{aligned}0 + T_R \;&=\; ux + T_R \;=\; \sum_{k=1}^{m} a_k\, ue(p_k,q_k) + T_R\\ &=\; \sum_{k=1}^{m} a_k\, e(up_k,q_k) + T_R \;=\; \Phi_u(x) + T_R\end{aligned}$$

That is $\Phi_u(x) \in T_R$ and hence $x = \Phi_{(1/u)}\Phi_u(x) \in T_R$ as $\Phi_{(1/u)}$ is an automorphism with $\Phi_{(1/u)}(T_R) \subseteq T_R$. That is $x \in T_R$ as well, such that $\mathrm{kn}(\overline{\beta}) \subseteq T_R \subseteq \mathrm{kn}(\overline{\beta})$. Then the first isomorphism theorem finally yields the following isomorphy

$$P_R \otimes_R Q_R \;=\; R^{\oplus(P\times Q)} \Big/ T_R \;\xrightarrow{\;\sim\;}\; S^{\oplus(P\times Q)} \Big/ T_S \;=\; P \otimes_S Q$$

Note that by construction as the isomorphy induced by $\overline{\beta}$ the element $p \otimes_R q = e(p,q) + T_R$ is mapped to $\overline{\beta}(e(p,q)) = f(p,q) + T_S = p \otimes_S q$. And as this map is κ-linear and bijective it truly is an isomorphism onto $P \otimes_S Q$ regared as an R-module.

(ii) **Remark:** If you did not like the lengthy, fundamental proof of (ii) above, note that in case of $M = R$ there is a more structural proof of this isomorphy. We start by $S \otimes_R U^{-1}N \xrightarrow{\;\sim\;} U^{-1}N$ using the R-bilinear map $S \times U^{-1}N \to U^{-1}N$ that maps $(a/u, y/v) \mapsto (ay)/(uv)$. By the universal property of the tensor product this map gives rise to a homomorphism of R-modules induced by

$$S \otimes_R U^{-1}N \;\to\; U^{-1}N \;:\; \frac{a}{u} \otimes_R \frac{y}{v} \;\mapsto\; \frac{ay}{uv}$$

Clearly this homomorphism is surjective and it remains to show its injectivity: For this we use that the general element of $S \otimes_R U^{-1}N$ can be written in the form (where $u := \prod_k u_k$ and $v := \prod_k v_k \in$

U and with $\widehat{u}_k := u/u_k$ and $\widehat{v}_k := v/v_k \in U$ we have $y := \sum_k a_k b_k \widehat{u}_k \widehat{v}_k y_k \in N$)

$$\begin{aligned}\sum_{k=1}^{m} b_k \left(\frac{a_k}{u_k} \otimes_R \frac{y_k}{v_k}\right) &= \sum_{k=1}^{m} b_k \left(\frac{a_k \widehat{u}_k}{u} \otimes_R \frac{\widehat{v}_k y_k}{v}\right) \\ &= \sum_{k=1}^{m} b_k \left(\frac{1}{u} \otimes_R \frac{a_k \widehat{u}_k \widehat{v}_k y_k}{v}\right) = \frac{1}{u} \otimes_R \frac{y}{v}\end{aligned}$$

Thereby $1/u \otimes_R y/v$ is mapped to y/uv and this equals $0/1 \in U^{-1}N$ if and only if $wy = 0$ for some $w \in U$. But from this we get

$$w\left(\frac{1}{u} \otimes_R \frac{y}{v}\right) = \frac{1}{u} \otimes_R \frac{wy}{v} = \frac{1}{u} \otimes_R \frac{0}{v} = 0$$

That is the kernel of this map is 0 and hence it is bijective, as well. The claim of (ii) in the case of $M = R$ now follows from (3.146.(i))

$$S \otimes_R U^{-1}N \xrightarrow{\sim} U^{-1}N \xrightarrow{\sim} S \otimes_S U^{-1}N$$

And thereby both $(a/u) \otimes_R (y/v)$ and $(a/u) \otimes_S (y/v)$ are mapped to the same element $(a/u)(y/v) = (ay)/(uv) \in U^{-1}N$, hence the isomorphism is induced by $(a/u) \otimes_R (b/v) \to (a/u) \otimes_S (y/v)$, as claimed.

(i) By (3.146.(iv)) we have the isomorphism $S \otimes M \xrightarrow{\sim} U^{-1}M$ induced by $(a/u) \otimes x \mapsto ax/u$. That is the preimage of $x/u \in U^{-1}M$ is $(1/u) \otimes x \in S \otimes M$. If we also apply this to $U^{-1}N$, then by (3.149.(iii)) we get the isomorphism

$$\begin{aligned}U^{-1}M \otimes U^{-1}N &\xrightarrow{\sim} (S \otimes M) \otimes (S \otimes N) \\ \frac{x}{u} \otimes \frac{y}{v} &\mapsto \left(\frac{1}{u} \otimes x\right) \otimes \left(\frac{1}{v} \otimes y\right)\end{aligned}$$

Due to the associativity and commutativity of the tensor product (3.144) we may rearrange this into the following form

$$\begin{aligned}U^{-1}M \otimes U^{-1}N &\xrightarrow{\sim} (S \otimes S) \otimes (M \otimes N) \\ \frac{x}{u} \otimes \frac{y}{v} &\mapsto \left(\frac{1}{u} \otimes \frac{1}{v}\right) \otimes (x \otimes y)\end{aligned}$$

Applying (ii) to $M = N = R$ we have the isomorphy $S \otimes_R S \xrightarrow{\sim} S$ under $a/u \otimes b/v \mapsto ab/uv$ such that by (3.150) we can continue with

$$\begin{aligned}U^{-1}M \otimes U^{-1}N &\xrightarrow{\sim} S \otimes (M \otimes N) \\ \frac{x}{u} \otimes \frac{y}{v} &\mapsto \frac{1}{uv} \otimes (x \otimes y)\end{aligned}$$

And by (3.146.(iv)) again we have the isomorpy of $S \otimes (M \otimes N)$ and $U^{-1}(M \otimes N)$ induced by $a/u \otimes (x \otimes y) \mapsto a(x \otimes y)/u$. Thus

$$U^{-1}M \otimes U^{-1}N \xrightarrow{\sim} U^{-1}(M \otimes N)$$

$$\frac{x}{u} \otimes \frac{y}{v} \quad \mapsto \quad \frac{x \otimes y}{uv}$$

□

Proof of (3.152):
The computational rules for the kronecker product of matrices could easily be proved by transferring them from the respective properties of R-module-homomorphisms (3.149). However we prefer to give direct, computational proofs of these equations as to be independent of the general theory of tensor-products. Let us start with $\mathbb{1}_m \in \mathrm{mat}_m(R)$ and $\mathbb{1}_n \in \mathrm{mat}_n(R)$. Then clearly the kronecker product $\mathbb{1}_m \otimes \mathbb{1}_n \in \mathrm{mat}_{mn}(R)$ and we can copute its coefficients by (where $i, j \in 1 \dots m$ and $k,l \in 1 \dots n$)

$$[\mathbb{1}_m \otimes \mathbb{1}_n]_{(i,k),(j,l)} \;=\; [\mathbb{1}_m]_{i,j}\,[\mathbb{1}_n]_{k,l} \;=\; \delta_{i,j}\delta_{k,l} \;=\; \delta_{(i,k),(j,l)} \;=\; [\mathbb{1}_{mn}]_{(i,k),(j,l)}$$

So altogether we have $\mathbb{1}_m \otimes \mathbb{1}_n = \mathbb{1}_{mn}$. Now consider the $(m \times n)$-matrices $A = (a_{i,j})$ and $C = (c_{i,j})$ as well as $(p \times q)$-matrices $B = (b_{k,l})$ and $D = (d_{k,l})$. If now $a, b \in R$ are scalars, then we find (since R is commutative)

$$\begin{aligned}
[A \otimes (bB + D)]_{(i,k),(j,l)} &= [A]_{i,j} \cdot [bB + D]_{k,l} \\
&= a_{i,j}\big(bb_{k,l} + d_{k,l}\big) \;=\; ba_{i,j}b_{k,l} + a_{i,j}d_{k,l} \\
&= b\,[A \otimes B]_{(i,k),(j,l)} + [A \otimes D]_{(i,k),(j,l)}
\end{aligned}$$

$$\begin{aligned}
[(aA + C) \otimes B]_{(i,k),(j,l)} &= [aA + C]_{i,j} \cdot [B]_{k,l} \\
&= \big(aa_{i,j} + c_{i,j}\big)b_{k,l} \;=\; aa_{i,j}b_{k,l} + c_{i,j}b_{k,l} \\
&= a\,[A \otimes B]_{(i,k),(j,l)} + [C \otimes B]_{(i,k),(j,l)}
\end{aligned}$$

Such that we get $A \otimes (bB + D) = b(A \otimes B) + A \otimes D$ and $(aA + C) \otimes B = a(A \otimes B) + C \otimes B$. And for the transpose matrices $A^* \in \mathrm{mat}_{n,m}(R)$ and $B^* \in \mathrm{mat}_{q,p}(R)$ we find that

$$\begin{aligned}
[A^* \otimes B^*]_{(j,l),(i,k)} &= [A^*]_{j,i} \cdot [B^*]_{l,k} \\
&= a_{i,j}b_{k,l} \;=\; [A \otimes B]_{(i,k),(j,l)} \\
&= [(A \otimes B)^*]_{(j,l),(i,k)}
\end{aligned}$$

such that $A^* \otimes B^* = (A \otimes B)^*$. Now consider an $(\ell \times m)$-matrix $A = (a_{i,j})$ and a $(m \times n)$-matrix $C = (c_{j,k})$. Then the product AC is the $(\ell \times n)$-matrix given by $[AC]_{i,k} = \sum_j a_{i,j}c_{j,k}$. Likewise for a $(p \times q)$-matrix $B = (b_{f,g})$ and an $(q \times r)$-matrix $D = (d_{g,h})$ the product BD is the $(p \times r)$-matrix with the coefficients $[BD]_{f,h} = \sum_g b_{f,g}d_{g,h}$. Now compute

$$\begin{aligned}
[(A \otimes B)(C \otimes D)]_{(i,f),(k,h)} &= \sum_{(j,g)=1}^{mq} [A \otimes B]_{(i,f),(j,g)}\,[C \otimes D]_{(j,g),(k,h)} \\
&= \sum_{(j,g)=1}^{mq} a_{i,j}b_{f,g}c_{j,k}d_{g,h}
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{j=1}^{m}\sum_{g=1}^{q} a_{i,j}c_{j,k}b_{f,g}d_{g,h} \\
&= \left(\sum_{j=1}^{m} a_{i,j}c_{j,k}\right)\left(\sum_{g=1}^{q} b_{f,g}d_{g,h}\right) \\
&= [AC]_{i,k}\cdot[BD]_{f,h} \\
&= [(AC)\otimes(BD)]_{(i,f),(k,h)}
\end{aligned}
$$

That is we have shown $(A\otimes B)(C\otimes D) = (AC)\otimes(BD)$. In particular we get $(A\otimes \mathbb{1}_p)(\mathbb{1}_n\otimes B) = (A\mathbb{1}_n)\otimes(\mathbb{1}_p B) = A\otimes B$. And if we return to the standard sizes $A = (a_{i,j}) \in \mathrm{mat}_{m,n}(R)$ and $B = (b_{k,l}) \in \mathrm{mat}_{p,q}(R)$ again, then a likewise computetion yields the equality $\mathrm{tr}(A\otimes B) = \mathrm{tr}(A)\cdot\mathrm{tr}(B)$

$$
\begin{aligned}
\mathrm{tr}(A\otimes B) &= \sum_{(i,k)=1}^{mp} [A\otimes B]_{(i,k),(i,k)} \\
&= \sum_{i=1}^{m}\sum_{k=1}^{q} a_{i,i}b_{k,k} \\
&= \left(\sum_{i=1}^{m} a_{i,i}\right)\left(\sum_{k=1}^{q} b_{k,k}\right) \\
&= \mathrm{tr}(A)\cdot\mathrm{tr}(B)
\end{aligned}
$$

□

Proof of (3.154):

(i) Let us first prove the case $n = 2$, that is we are given two E-modules M and N and some elements $x \in M$ and $y \in N$. If $x = 0$, then it is clear that

$$
\begin{aligned}
x\otimes y &= 0_M\otimes y = (0\cdot 0_M)\otimes y \\
&= 0\cdot(0_M\otimes y) = 0_M\otimes(0\cdot y) = 0_M\otimes 0_N = 0
\end{aligned}
$$

and likewise $y = 0$ implies $x\otimes y = 0$. If remains to prove the inverse implication, that is we have $x\otimes y = 0$ and need to show $x = 0$ or $y = 0$. To do this pick up bases $\{ m_i \mid i\in I\}$ of M and $\{ n_j \mid j\in J\}$ of N. Then we find a basis representation $x = \sum_i a_i m_i$ and $y = \sum_j b_j n_j$ where the sums are finite only. Then we see that

$$
0 = x\otimes y = \left(\sum_{i\in I} a_i m_i\right)\otimes\left(\sum_{j\in J} b_j n_j\right) = \sum_{i\in I}\sum_{j\in J} a_i b_j\, m_i\otimes n_j
$$

But in (3.146.(v)) we have seen, that the $m_i\otimes n_j$ form a basis of $M\otimes N$. Therefore for any $i\in I$ and any $j\in J$ the coefficient $a_i b_j = 0$ has to vanish. If $x\neq 0$ then there is some $r\in I$ such that $a_r = 0$ and therefore $a_r b_j = 0$ implies $b_j = 0$ for all $j\in J$. That is we have $y = 0$ (or $x = 0$) as claimed. In case of general $n\geq 3$ we use induction, taking to $M := M_1$, $x := x_1$ and $N := M_2\otimes\ldots\otimes M_n$ resp. to $y := x_2\otimes\ldots\otimes x_n$. Then the tensor product's associativity (3.144.(ii)) $M_1\otimes\ldots\otimes M_n \xrightarrow{\sim} M\otimes N : x_1\otimes\ldots\otimes x_n \mapsto x\otimes y$ turns the assumption $x_1\otimes\ldots\otimes x_n = 0$ into $x\otimes y = 0$ which is equivalent to $x_1 = x = 0$ or $y = 0$. And by induction hypothesis $y = 0$ is

equivalent to one of the x_2 to x_n being zero, as well.

(ii) As in (i) above, let us first prove the case $n = 2$, that is we are given two E-modules M and N and some elements u, $v \in M$ and x, $y \in N$ such that $u \otimes x = v \otimes y \neq 0$. We now pick up bases $\{ m_i \mid i \in I \}$ of M and $\{ n_j \mid j \in J \}$ of N again denote the basis representation of these elements, by $u = \sum_i u_i m_i$, $v = \sum_i v_i m_i$ and $x = \sum_j x_j n_j$, $y = \sum_j y_j n_j$ respectively. Then (as before) $u \otimes x = v \otimes y$ is nothing but $\sum_{i,j} u_i x_j \, m_i \otimes n_j = \sum_{i,j} v_i y_j \, m_i \otimes n_j$ which in turn is $u_i x_j = v_i y_j$ for all $i \in I$ and $j \in J$. We can even multiply this equation with some $\omega_i \in E$ to find $\omega_i u_i x_j = \omega_i v_i y_j$. Summing up all these equations over i yields $\langle (\omega_i) \mid (u_i) \rangle x_j = \langle (\omega_i) \mid (v_i) \rangle y_j$ and as this is true for all $j \in J$ we get $\langle (\omega_i) \mid (u_i) \rangle x = \langle (\omega_i) \mid (v_i) \rangle y$. By assumption we also have $v \otimes y \neq 0$ which by (i) implies $v \neq 0$ (and $y \neq 0$). Therefore we have $(v_i) \neq 0$ such that there is some $(\omega_i) \in E^I$ such that $\langle (\omega_i) \mid (v_i) \rangle \neq 0$. Letting $b := \langle (\omega_i) \mid (u_i) \rangle / \langle (\omega_i) \mid (v_i) \rangle$ for this (ω_i) we hence get $y = bx$. In complete analogy we can find some $a \in E$ such that $v = au$. Now compute

$$u \otimes v \;=\; v \otimes y \;=\; (au) \otimes (bx) \;=\; ab\,(u \otimes x)$$

which is $(ab - 1)(u \otimes v) = 0$. Using (i) and the assumption $u \otimes x \neq 0$ this also implies $ab = 1$. As in (i) we use induction for the general case $n \geq 3$ using the same notation as above $u := x_1$, $x := x_2 \otimes \ldots \otimes x_n$, $v := y_1$ and $y := y_2 \otimes y_n$. Then the assumption $x_1 \otimes \ldots \otimes x_n = y_1 \otimes \ldots \otimes y_n$ turns into $u \otimes x = v \otimes y$ from which we get $v = a_1 u$ and $y = a_2 x$ for some a_1 and $a_2 \in R$ with $a_1 a_2 = 1$. Letting $z := a_2 x = (a_2 x_2) \otimes x_3 \otimes \ldots x_n$ we get $y = z$ which by induction hypothesis yields some $b_i \in R$ such that $y_2 = b_2 z_2 = b_2 a_2 x_2$ and $y_i = b_i z_i = b_i x_i$ for $i \in 3 \ldots n$ with $b_2 \ldots b_n = 1$. Multiplying all the coefficients we find $a_1 (b_2 a_2) b_3 \ldots b_n = (a_1 a_2)(b_2 \ldots b_n) = 1$, as claimed.

(iii) Let $X_i = \{ x_{i,k} \mid k \in K(i) \}$ for some index set $K(i) \neq \emptyset$. And for any $i \in 1 \ldots n$ let us regard the canonical homomorphism

$$\varrho_i : R^{\oplus K(i)} \to M_i \;:\; (a_k) \mapsto \sum_{k \in K(i)} a_k x_{i,k}$$

Let us also abbreviate $X := X_1 \otimes \ldots \otimes X_n$ and the tensor products of $M := M_1 \otimes \ldots \otimes M_n$ and of these homomorphisms by $\varrho := \otimes_1 \otimes \ldots \otimes \varrho_n$. Then X_i generates M_i iff ϱ_i is surjective. But in this case we see that ϱ is surjective again, due to (3.149.(iv)) which means that X generates M. Likewise X_i is linear independent iff ϱ_i is injective. And in this case ι is injective again, since E is a field and we have (3.149.(iv)) again. But this is nothing but the linear independence of X. Finally X_i is a basis of M_i iff ϱ_i is bijective. And in this case (3.149.(iv)) again implies, that ϱ is bijective, such that X is a basis of M.

(vi) Pick up a basis $\{ n_j \mid j \in J \}$ of N and for each y_k and $y'_k \in N$ pick up basis representations $y_k = \sum_j a_{j,k} n_j$ and $y'_k = \sum_j a'_{j,k} n_j$ respectively. Then we compute

$$\sum_{j \in J} \sum_{k=1}^{m} a_{j,k} \, x_k \otimes n_j \;=\; \sum_{k=1}^{m} x_k \otimes y_k \;=\; \sum_{k=1}^{m} x_k \otimes y'_k \;=\; \sum_{j \in J} \sum_{k=1}^{m} a'_{j,k} \, x_k \otimes n_j$$

But as the x_k and n_j are lineary independent we know by (iii) that the tensors $x_k \otimes n_j$ are linear

independent in $M \otimes N$. And hence we get $a_{j,k} = a'_{j,k}$ for any $j \in J$ and $k \in 1 \dots m$. But that is $y_k = y'_{j,k}$ for any $k \in 1 \dots m$ again, as had been claimed.

(iv) Take a look at the embeddings $\iota_i : U_i \hookrightarrow M_i : x_i \mapsto x_i$, as these are injective and E is a field we find that $\iota_1 \otimes \dots \otimes \iota_n$ is injective again, according to (3.149.(iii)). In particular we get the explicit representation of $U_1 \otimes \dots \otimes U_n$ as a subset of $M_1 \otimes \dots \otimes M_n$

$$\bigotimes_{i=1}^{n} U_i = \left\{ \sum_{k=1}^{m} a_k \, u_{1,k} \otimes \dots \otimes u_{n,k} \;\middle|\; a_k \in E, u_{i,k} \in M_i \right\} \subseteq \bigotimes_{i=1}^{n} M_i$$

The equality for the intersection of subspaces will use inducion on n and will be require the use of (vii). Hence it is proved after that.

(v) The implication " $\Longleftarrow$ " is clear by the explicit representation of the product $U_1 \otimes \dots \otimes U_n$ as a subset of $M_1 \otimes \dots \otimes M_n$ that has been given in (iv). And in the direction " $\Longrightarrow$ " we will only prove $x_{1,k} \in M_1$ for ease of notation. The other cases ($i \in 2 \dots n$) can be shown in complete analogy. So let us denote $M := M_1$ and $N := M_2 \otimes \dots \otimes M_n$ as well as $x_k := x_{1,k} \in M$ and $y_k := x_{2,k} \otimes \dots \otimes x_{n,k} \in N$. Note that according to (iii) $\{ y_1, \dots, y_m \}$ is linear independent again. And we also have the natural isomorphy $M_1 \otimes \dots \otimes M_n \xrightarrow{\sim} M \otimes N : x_{1,k} \otimes \dots \otimes x_{n,k} \mapsto x_k \otimes y_k$. Let us finally abbreviate $U := U_1 \leq_{\mathrm{v}} M$ and $V := U_2 \otimes \dots \otimes U_n \leq_{\mathrm{v}} V$ and regard the canonical homomorphism

$$\varrho \;:\; M \twoheadrightarrow {}^{M}\!/_{U} \;:\; x \mapsto x + U$$

Then $\varrho \otimes N : M \otimes N$ is defined by $x \otimes y \mapsto (x + U) \otimes y$. Using this homomorphism on $t = \sum_k a_k x_k \otimes y_k$ we get

$$\begin{aligned} (\varrho \otimes N)(t) &= (\varrho \otimes N) \left(\sum_{k=1}^{m} a_k \, x_k \otimes y_k \right) \\ &= \sum_{k=1}^{m} a_k (x_k + U) \otimes y_k \;=\; \sum_{k=1}^{m} (a_k x_k + U) \otimes y_k \end{aligned}$$

But by assumption we also have $t \in U_1 \otimes \dots \otimes U_n = U \otimes V$ such that there are some $b_r \in E$ $u_r \in U$ and $v_r \in V$ (where $r \in 1 \dots s$) such that $t = \sum_r b_r u_r \otimes v_r$. Using $\varrho \otimes N$ on t again, this time we find

$$\begin{aligned} (\varrho \otimes N)(t) &= (\varrho \otimes N) \left(\sum_{r=1}^{s} b_r \, u_r \otimes v_r \right) \\ &= \sum_{r=1}^{s} b_r (u_r + U) \otimes v_r \;=\; \sum_{r=1}^{s} b_r (u_r + U) \otimes v_r \\ &= \sum_{r=1}^{s} b_r (0 + U) \otimes v_r \;=\; 0 \;=\; \sum_{k=1}^{m} (0 + U) \otimes y_k \end{aligned}$$

As the y_k are linear independent (vi) now tells us, that for any index $k \in 1 \dots m$ we get $a_k x_k + U = 0 + U$ which is $a_k x_k \in U$. But as $a_k \neq 0$ and E is a field this yields $x_{1,k} = x_k \in U = U_1$ as claimed.

(vii) For the implication " $\Longrightarrow$ " let us suppose $\{ x_1, \dots, x_m \}$ was *not* linear independent, then we have

to prove that m is *not* minimal Without loss of generality (and for ease of notation) let us assume that

$$x_1 \;=\; \sum_{k=2}^{m} b_k x_k$$

for some $b_k \in E$. Then we could rearrange t is such a way as to reduce the number of pure tensors required to build up t

$$\begin{aligned} t \;&=\; \sum_{k=1}^{m} a_k\, x_k \otimes y_k \;=\; a_1\, x_1 \otimes y_1 + \sum_{k=2}^{m} a_k\, x_k \otimes y_k \\ &=\; a_1 \left(\sum_{k=2}^{m} b_k x_k \right) \otimes y_1 + \sum_{k=2}^{m} a_k\, x_k \otimes y_k \\ &=\; \sum_{k=2}^{m} x_k \otimes (a_1 b_k y_1) + \sum_{k=2}^{m} x_k \otimes (a_k y_k) \\ &=\; \sum_{k=2}^{m} x_k \otimes (a_1 b_k y_1 + a_k y_k) \end{aligned}$$

Thus we have discounted the minimality of m by showing $\mu(t) \leq m-1 < m$. Hence the assumption of the linear independance of $\{\, x_1, \ldots, x_m \,\}$ must be false. The case that $\{\, y_1, \ldots, y_m \,\}$ is not linearly independent can be shown in complete analogy. And if $a_k = 0$ then $x_k \otimes y_k$ can be omitted for trivial reasons. For the converse implication " $\Longleftarrow$ " we are given a representation of t with $b_r \neq 0$ and linearly independent $\{\, u_1, \ldots, u_s \,\} \subseteq M$ and $\{\, v_1, \ldots, v_s \,\} \subseteq N$

$$t \;=\; \sum_{r=1}^{s} b_r\, u_r \otimes v_r$$

Let us denote $U := \mathrm{Lh}\{\, u_1, \ldots, u_s \,\} \;\leq_{\mathrm{v}}\; M$ and $V := \mathrm{Lh}\{\, v_1, \ldots, v_s \,\} \;\leq_{\mathrm{v}}\; N$ and consider an arbitrary representation of t in terms of

$$t \;=\; \sum_{k=1}^{m} a_k\, x_k \otimes y_k$$

Then we have to show that $s \leq m$ such that $\mu(t) = s$. Without loss of generality we can also assume $a_k \neq 0$, as this would only increase the number m of pure tensors used. Then the u_r are linearly independent we may append them to a basis $\{\, u_1, \ldots, u_s \,\} \subseteq \{\, u_i \mid i \in I \,\}$ of M. And likewise let $\{\, v_1, \ldots, v_s \,\} \subseteq \{\, v_j \mid j \in J \,\}$ be a basis of N. Then we express the x_k as linear combinations of this basis likewise

$$x_k \;=\; \sum_{i \in I} x_{i,k} u_i \quad \text{and} \quad y_k \;=\; \sum_{j \in J} y_{i,k} v_i$$

Inserting these representations we obtain the following expression of t

$$t \;=\; \sum_{k=1}^{m} a_k\, x_k \otimes y_k \;=\; \sum_{i \in I} \sum_{j \in J} \left(\sum_{k=1}^{m} a_k x_{i,k} y_{j,k} \right) u_i \otimes v_j$$

Note that according to (iii) $\{\, u_i \otimes y_j \mid i \in I, j \in J \,\}$ is a basis of $M \otimes N$. So comparing this representation of t with the one we started with $t = \sum_r b_r u_r \otimes v_r$ we see that for $1 = j = r \in 1 \ldots s$ we

get

$$\sum_{k=1}^{m} a_k x_{r,k} y_{r,k} \;=\; b_r$$

And in case $i \neq j$ (or $i = j \notin 1 \ldots s$ which is of no interest to us however) we likewise see, that

$$\sum_{k=1}^{m} a_k x_{i,k} y_{j,k} \;=\; 0$$

Recall that $b_r \neq 0$ so we may divide the above equation by b_r (also note that thereby $j = r$). So if we denote $p_{k,j} := a_k b_j^{-1} y_{j,k}$ then for any $i, j \in 1 \ldots s$ we altogether find the equality

$$\sum_{k=1}^{m} x_{i,k} p_{k,j} \;=\; \sum_{k=1}^{m} x_{i,k} a_k b_j^{-1} y_{j,k} \;=\; b_j^{-1} \sum_{k=1}^{m} a_k x_{i,k} y_{j,k} \;=\; \delta_{i,j}$$

Thus if we take to the $(m \times s)$-matrix $P := (p_{k,i})$ and to the $(s \times m)$-matrix $X := (x_{i,k})$ over E the above equations turn into nothing but the matrix equation $XP = \mathbb{1}_s$. In particular if we regard P as a linear map $P : R^s \hookrightarrow R^m$ it is injective. And due to dimension reasons this implies $s \leq m$, so s is minimal indeed.

(v) (continued) We will now prove the equality for the intersection of subspaces, that has been postponed so far. The containment "$\subseteq$" is easy to see, just let us abbreviate $U_i := \bigcap_j U_{i,j}$ and consider some $t \in U_1 \otimes \ldots \otimes U_n$. That is $t = \sum_k a_k u_{1,k} \otimes \ldots \otimes u_{n,k}$ for some $u_{i,k} \in U_i$. But as $U_i \subseteq U_{i,j}$ for all $j \in J(i)$ this is $u_{i,k} \in U_{i,j}$ for any $i \in 1 \ldots n$, $j \in J(i)$ and $k \in 1 \ldots m$ such that $t \in U_{1,j(1)} \otimes \ldots \otimes U_{n,j(n)}$ for any $j \in J(1) \times \cdots \times J(n)$ again. Hence t is contained in the intersection of these spaces, as claimed. For the converse inclusion "$\supseteq$" we will use induction on n. First consider the case $n = 2$, that is we are given two E-vectorspaces M and N and families of subspaces $U_i \leq_{\mathrm{v}} M$ and $V_j \leq_{\mathrm{v}} N$ where $i \in I$ and $j \in J$ respectively. Then we have to prove

$$\bigcap_{(i,j) \in I \times J} U_i \otimes V_j \;\subseteq\; \left(\bigcap_{i \in I} U_i \right) \otimes \left(\bigcap_{j \in J} V_j \right)$$

Thus consider some $t \in \bigcap_{(i,j)} U_i \otimes V_j$ that is for any $i \in I$ and any $j \in J$ there are some $a_r(i,j) \in E$, $u_r(i,j) \in U_i$ and $v_r \in V_j$ (where $r \in 1 \ldots s(i,j)$ such that

$$t \;=\; \sum_{k=1}^{s(i,j)} a_r(i,j)\, u_r(i,j) \otimes v_r(i,j)$$

According to (vii) we may take the $a_r(i,j) \neq 0$ and the $u_r(i,j) \in M$ respectively the $v_r(i,j) \in N$ to be E-linearly independent. Now fix any $p \in I$ and $q \in J$ and recall that we still have $t \in U_i \otimes V_j$ then

$$t \;=\; \sum_{k=1}^{s(p,q)} a_r(p,q)\, u_r(p,q) \otimes v_r(p,q) \;\in\; U_i \otimes V_j$$

Then (v) implies that $u_r(p,q) \in U_i$ and $v_r(p,q) \in V_j$ for any $i \in I$ and any $j \in J$ respectively. That is they are contained in the intersection $u_r(p,q) \in U := \bigcap_i U_i$ and $v_r(p,q) \in V := \bigcap_j V_j$ respectively. But this again implies $t \in U \otimes V$ as claimed. For the induction step $n \geq 3$ let us

denote $M := M_1$ and $N := M_2 \otimes \ldots \otimes M_n$ again. Likewise $I := J(1)$ and $J := J(2) \times \cdots \times J(n)$ and $U_i := U_{1,i}$ for $i \in I$ and finally $V_j := U_{2,j(2)} \otimes \ldots \otimes U_{n,j(n)}$ for $j = (j(2), \ldots, j(n)) \in J$ respectively. Then by induction hypothesis we have

$$\bigcap_{j\in J} V_j \;=\; \bigcap_{j\in J(2)\times\cdots\times J(n)} \bigotimes_{i=2}^{n} U_{i,j(i)} \;\subseteq\; \bigotimes_{i=2}^{n} \left(\bigcap_{j\in J(i)} U_{i,j} \right)$$

But in the case $n = 2$ we have just shown that also $\bigcap_{i,j} U_i \otimes V_j \subseteq (\bigcap_i U_i) \otimes (\bigcap_j V_j)$. Thus we may compute

$$\begin{aligned} \bigcap_{i,j} U_i \otimes V_j &\subseteq \left(\bigcap_{i\in I} U_i \right) \otimes \left(\bigcap_{j\in J} V_j \right) \\ &\subseteq \left(\bigcap_{i\in I} U_i \right) \otimes \left(\bigotimes_{i=2}^{n} \left(\bigcap_{j\in J(i)} U_{i,j} \right) \right) \\ &= \bigotimes_{i=1}^{n} \left(\bigcap_{j\in J(i)} U_{i,j} \right) \end{aligned}$$

□

Proof of (3.160):

(i) If M is free with basis $\{ m_i \mid i \in I \}$ then according to (3.146.(iv)) we obtain the following isomorphy of R-modules

$$\Phi \;:\; S^{\oplus I} \;\xrightarrow{\sim}\; M_S \;:\; (s_i) \mapsto \sum_{i\in I} s_i \otimes m_i$$

But Φ clearly not only is R-linear, but even S-linear, as $\Phi(a(s_i)) = \Phi(as_i) = \sum_i (as_i) \otimes m_i = \sum_i a(s_i \otimes m_i) = a \sum_i s_i \otimes m_i = a\Phi(s_i)$. Also $\Phi(s_i)$ is nothing but an S-linear combination of the $1_S \otimes m_i$

$$\Phi\big((s_i)\big) \;=\; \sum_{i\in I} s_i \, (1_S \otimes m_i)$$

That is Φ is precisely the canonical homomorphism $S^{\oplus I}$ onto the linear combinations of the $\{ 1_S \otimes m_i \mid i \in I \} \subseteq M$. And its bijectivity proves that this set truly is an S-basis of M_S.

(ii) We have just seen in (i) that $\{ 1_S \otimes m_i \mid i \in 1 \ldots m \}$ truly is an R-basis of M_S and likewise for N_S. The identity of the matrix representation of φ boils down to a vey short, straightforward computation:

$$\begin{aligned} \varphi_S(1_S \otimes m_j) &= 1_S \otimes \varphi(m_j) \;=\; 1_S \otimes \left(\sum_{i=1}^{m} a_{i,j} n_i \right) \\ &= \sum_{i=1}^{m} a_{i,j} \, 1_S \otimes n_i \;=\; \sum_{i=1}^{m} (a_{i,j} 1_S) \, (1_S \otimes n_i) \end{aligned}$$

(iii) As S is a free R-algebra with $S \neq 0$ we have seen in (3.52.(ii)) that the canonical map $\iota : R \hookrightarrow S : a \mapsto a1_S$ is injective and that there is some sub-module $S' \leq_{\mathsf{m}} S$ such that $S = (S1_S) \oplus S'$.

That is $\mathrm{im}(I) \oplus S' = S$ such that by (3.149.(iv)) we find that $\iota_S := \iota \oplus M : R \otimes M \hookrightarrow S \otimes M$ is injective again. Thereby ι_S is defined by linear expansion of $\iota_S(a \otimes x) = (a1_S) \otimes x$. But due to the isomorphy $\Lambda : R \otimes M \xrightarrow{\sim} M : a \otimes x \mapsto ax$ we can shift ι_S to M, where we get

$$\iota_S \Lambda^{-1} \ : \ M \hookrightarrow M_S \ : \ x \mapsto 1_S \otimes x$$

If the reader is not entirely convinced by this just fix some $x, y \in M$ and compute: $1_S \otimes x = 1_S \otimes y$ is nothing but $\iota_S(1 \otimes x) = \iota_S(1 \otimes y)$. But as ι_S is injective, this means $1 \otimes x = 1 \otimes y$. Now the isomorphy Λ yields $x = \Lambda(1 \otimes x) = \Lambda(1 \otimes y) = y$ which had to be shown.

(iv) Clearly $B \times M_A \to M_B : (b, t) \mapsto bt$ is a bilinear map, such that by the universal property of the tensor-product we find a well-defined homomorphism of A modules, by

$$\Phi \ : \ \left(M_A\right)_B = B \otimes M_A \to M_B \ : \ b \otimes t \mapsto bt$$

On the other hand we clearly get another bilinear map by taking to $B \times M \to (M_A)_B : (b, x) \mapsto b \otimes (1_A \otimes x)$. And by the universal property of the tensor-product again, this yields another well-defined homomorphism of A modules, by

$$\Psi \ : \ M_B = B \otimes M \to \left(M_A\right)_B \ : \ b \otimes x \mapsto b \otimes (1_A \otimes x)$$

And it is easy to see that these maps are mutual inverse of on and another. It suffices to check this on the generating set of pure tensors: $\Phi\Psi(b \otimes x) = \Phi(b \otimes (1_A \otimes x)) = (1_A b) \otimes x = b \otimes x$ and conversely $\Psi\Phi(b \otimes (a \otimes x)) = \Psi(b(a \otimes x)) = \Psi(ab \otimes x) = ab \otimes (1_A \otimes x) = b \otimes (a \otimes x)$. Note that we thereby used the definition of the scalar multiplication in $(M_A)_B$ which is $b(a \otimes x) = ab \otimes x$. Hence Φ is an isomorphism of A-modules, but as it is B-linear as well, we even have an isomorphy of B-modules.

(vi) Let us first prove the well-definedness of $\varphi(S)$. To do this regard the map $S \times M \to s\varphi(x)$. The R-linearity in the first argument is obvious: $(r + s, x) \mapsto (r + s)\varphi(x) = r\varphi(x) + s\varphi(x)$ and $(as, x) \mapsto (as)\varphi(x) = (a1_S s)\varphi(x) = (a1_S)(s\varphi(x)) = a(s\varphi(x))$. Before we proceed with the R-linearity in the second argument recall, that for any $a \in R$ and $s \in S$ we get $(a1_S)s = a(1_S s) = a(s1_S) = s(a1_S)$ since S is an R-algebra. That is $a1_S$ commutes with any $s \in S$. Using this we can compute $(s, x + y) \mapsto s\varphi(x + y) = s(\varphi(x) + \varphi(y)) = s\varphi(x) + s\varphi(y)$ and $(s, ax) \mapsto s\varphi(ax) = s(a1_S)\varphi(x) = (a1_S)s\varphi(x) = a(s\varphi(x))$. Hence by the universal property of tensor products (3.142) we find an R-linear map, defined by linear expansion of

$$\varphi_{(S)} \ : \ S \otimes M \to N \ : \ s \otimes x \mapsto s\varphi(x)$$

Let us now prove that $\varphi \mapsto \varphi_{(S)}$ and $\psi \mapsto (x \mapsto \psi(1_S \otimes x))$ truly are mutually inverse maps (this also proves the uniqueness part of the claim). The one direction is trivial, as $\varphi_{(S)}$ has been constructed using $\varphi_S(1_S \otimes x) = \varphi(x)$. And if we start with $\psi : M_S \to N$ let us define $\varphi(x) := \psi(1_S \otimes x)$. Clearly $\varphi : M \to N$ is R-linear and we get

$$\varphi_{(S)}(s \otimes x) \ = \ s\varphi_{(S)}(1_S \otimes x) \ = \ s\psi(1_S \otimes x)$$

$$= \quad \psi\big(s(1_S \otimes x)\big) = \psi(s \otimes x)$$

In particular $\varphi \mapsto \varphi_{(S)}$ is bijective, but this map also is R-linear, as we may easily compute $(\varphi + \varphi')_{(S)}(s \otimes x) = s(\varphi + \varphi')(x) = s(\varphi(x) + \varphi'(x)) = s\varphi(x) + s\varphi'(x) = \varphi_{(S)}(s \otimes x) + \varphi'_{(S)}(s \otimes x)$ and for $a \in R$ also $(a\varphi)_{(S)}(s \otimes x) = s(a\varphi(x)) = a(s\varphi(x)) = a\varphi_{(S)}(s \otimes x)$. And if S is commutative then for r, $s \in S$ we may also compute $(r\varphi)_{(S)}(s \otimes x) = s(r\varphi(x)) = (sr)\varphi(x) = (rs)\varphi(x) = r(s\varphi(x)) = r\varphi_{(S)}(s \otimes x)$. So in this case $\varphi_{(S)}$ even is S-linear.

(vii) As in particular A is an R-module and B is an S-module we have already seen in (iv), that $\varphi_{(S)} : A \to B$ is a well-defined, S-linear map. It remains to verify the multiplicativity of $\varphi_{(S)}$. But due to the S-linearity it suffices to do this on the generating set of pure tensors:

$$\begin{aligned}
\varphi_{(S)}\big((r \otimes x)(s \otimes y)\big) &= \varphi_{(S)}\big((rs) \otimes (xy)\big) \;=\; (rs)\varphi(xy) \\
&= r(s\varphi(xy)) \;=\; r\big(s(\varphi(x)\varphi(y))\big) \\
&= r\big(\varphi(x)(s\varphi(y))\big) \;=\; (r\varphi(x))(s\varphi(y)) \\
&= \varphi_{(S)}(r \otimes x)\varphi_{(S)}(s \otimes y)
\end{aligned}$$

And if A and B both contain an unit element and φ is a homomorphism of R-algebras [that is $\varphi(1_A) = 1_B$] we find that $\varphi_{(S)}(1_S \otimes 1_A) = 1_S\varphi(1_A) = 1_S 1_B = 1_B$. As $1_S \otimes 1_A$ is the unit element of A_S this also proves that $\varphi_{(S)}$ is a homomorphism of S-algebras.

(v) Let us abbreviate the R-module $M := M(1) \otimes_R \ldots \otimes_R M(n)$ and the N-module $N := M(1)_S \otimes_S \ldots \otimes_S M(n)_S$. Then we need to show the isomorphy $M_S \xrightarrow{\sim} N$. To do this we stert with the following R-multilinear map

$$\prod_{i=1}^{n} M(i) \to N \;:\; (x_1, \ldots, x_n) \mapsto (1_S \otimes x_1) \otimes \ldots \otimes (1_S \otimes x_n)$$

Due to the multilinearity and the universal property of tensor products this map induces an R-linear map η, which is of the form

$$\eta \;:\; M \to N \;:\; x_1 \otimes \ldots \otimes x_n \mapsto (1_S \otimes x_1) \otimes \ldots \otimes (1_S \otimes x_n)$$

That is we have to show that $\eta_{(S)} : M_S \to N$ truly is an isomorphism of S-modules. And to do this we will construct the inverse map: first of all take a look at the product map $S^n \to S : (s_1, \ldots, s_n) \mapsto \prod_i s_i$. This map clearly is S-multilinear and hence induces an S-linear map

$$\mu \;:\; S^{\otimes n} \to S \;:\; s_1 \otimes s_n \mapsto \prod_{i=1}^{n} s_i$$

We will now compose the tensor mapping $\tau : M(1)_S \times \cdots \times M(n)_S \to M(1)_S \otimes_R \ldots \otimes_R M(n)_S$ and the isomorphy of the associativity of the tensor product (3.144.(ii)) $M(1)_S \otimes_R \ldots \otimes_R M(n)_S \xrightarrow{\sim} S^n \otimes_R M$ with $\mu \otimes M : S^n \otimes_R M \to S \otimes_R M$ to finally find the following map

$$M(1)_S \times \cdots \times M(n)_S \to S \otimes_R M$$

$$(s_1 \otimes x_1, \ldots, s_n \otimes x_n) \mapsto \left(\prod_{i=1}^{n} s_i\right) \otimes (x_1 \otimes \ldots \otimes x_n)$$

Looking at the explicit definition of this map it is clear that it is S-multilinear and thereby induces an S-linear map $\pi : N \to M_S$, by S-linear expansion of

$$\pi \ : \ (s_1 \otimes x_1) \otimes \ldots \otimes (s_n \otimes x_n) \mapsto \left(\prod_{i=1}^{n} s_i\right) \otimes (x_1 \otimes \ldots \otimes x_n)$$

From the explicit construction of this map it is clear, that π is the inverse of $\eta_{(S)} : 1_S \otimes (x_1 \otimes \ldots \otimes x_n) \mapsto (1_S \otimes x_1) \otimes \ldots \otimes (1_S \otimes x_n)$. Hence $\eta_{(S)}$ is bijective, that is an isomorphism of S-modules.

□

Proof of (3.161):

(iii) Let $\{ u_i \mid i \in I \} \subseteq U$ be an E-basis of $\mathsf{kn}(\varphi)$ and $\{ v_j \mid j \in J \} \subseteq V$ be an E-basis of $\mathsf{im}(\varphi)$. For any $i \in J$ we pick up some $x_j \in U$ such that $\varphi(x_j) = v_j$. Hence $\{ u_i \mid i \in I \} \cup \{ x_j \in j \in J \}$ is an E-basis of U due to the first isomorphism theorem

$$U \Big/ _{\mathsf{kn}(\varphi)} \ \xrightarrow{\sim} ; \mathsf{im}(\varphi) \ : \ x + \mathsf{kn}(\varphi) \mapsto \varphi(x)$$

To see this consider some $x \in U$, then $\varphi(x) = \sum_j b_j v_j = \sum_j b_j \varphi(x_j) = \varphi(\sum_j b_j x_j)$ for some uniquely determined $b_j \in E$. But this implies $\varphi(u - \sum_j b_j x_j) = 0$ such that $u - \sum_j b_j x_j \in \mathsf{kn}(\varphi)$. Therefore there are uniquely determined $a_i \in E$ such that $u - \sum_j b_j x_j = \sum_i a_i u_i$. Altogether we have found a unique linear combination of any $x \in U$, which means that $\{ u_i \mid i \in I \} \cup \{ x_j \in j \in J \}$ is an E-basis of U. And according to (3.160.(i)) we find that $\{ 1_S \otimes u_i \mid i \in I \} \cup \{ 1_S \otimes x_j \in j \in J \}$ is an S-basis of U_S. But it is clear, that

$$\begin{aligned} \varphi_S(1_S \otimes u_i) &= 1_S \otimes \varphi(u_i) = 0 \\ \varphi_S(1_S \otimes x_j) &= 1_S \otimes \varphi(x_f) = 1_S \otimes v_j \end{aligned}$$

In particular $\mathsf{im}(\varphi_S) = \varphi_S(U_S) = \mathsf{Lh}_S\{ 1_S \otimes v_j \mid j \in J \}$. And as the set $\{ 1_S \otimes v_j \mid j \in J \}$ is a basis, it is a S-linear independent set that generates $\mathsf{im}(\varphi_S)$, hence a S-basis.

(ii) We continue with the reasoning of (iii) above: Since $\{ 1_S \otimes u_i \mid i \in I \}$ is part of an S-basis of U_S, as well, it has to be S-linearly independent. Now consider any $u_S \in \mathsf{kn}(\varphi_S) \subseteq U_S$. Then we can write u_S in the following form

$$u_S = \sum_{i \in I} a_i 1_S \otimes u_i + \sum_{j \in J} b_j 1_S \otimes x_j$$

for some (uniquely determined) a_i and $b_j \in S$. By applying φ_S to this equation we find $0 = \varphi_S(u_s) = \sum_{j \in J} b_j 1_S \otimes v_j$. And as the $1_S \otimes v_j$ are S-linearly independent, this means $b_j = 0$ for any $j \in J$. That is $u_S = \sum_{i \in I} a_i 1_S \otimes u_i$ and as u_S has been chosen arbitarily, this means:

$$\mathsf{kn}(\varphi_S) = \mathsf{Lh}_S\{ 1_S \otimes u_i \mid i \in I \}$$

That is the set $\{ 1_S \otimes u_i \mid i \in I \}$ is an S-linearly independent set, that generates $\mathrm{kn}(\varphi_S)$, hence a basis.

(i) Since φ_S is injective if and only if $\mathrm{kn}(\varphi_S) = 0$, which according to (ii) is equivalent to $\mathrm{kn}(\varphi) = 0$, which in turn is equivalent to φ being injective, we have proved the equivalence of injectivity.

And as φ_S is surjective if and only if $\mathrm{im}(\varphi_S) = V_S$, which according to (iii) is equivalent to $\mathrm{im}(\varphi) = V$, which in turn is equivalent to φ being surjective, we have proved the equivalence of surjectivity, as well.

(iv) By definition the rank of a linear map is the dimension of the image of the map. Now in (iii) we have seen, that $\mathrm{im}(\varphi)$ and $\mathrm{im}(\varphi_S)$ both have bases of the common cardinality $|J|$. In particular, they share the same dimension $|J|$.

□

Proof of (3.159):
The first three isomorphies have been proved in (3.146) already. Also note that the proof of the remaining two isomorphies requires the use of (3.160) which has been proved right before these assertions here.
Polynomials: Clearly $\{ t^\alpha \mid \alpha \in A \}$ is an R-basis of $R[t \mid A]$ such that by (3.160.(i)) $\{ 1_S \otimes t^\alpha \mid \alpha \in A \}$ is an S-basis of $R[t \mid A]_S$. But $\{ t^\alpha \mid \alpha \in A \}$ also is an S-basis of $S[t \mid A]$, so we may define the following isomorphy of S-modules, by S-linear expansion from the basis

$$\Phi \ : \ S\,[t \mid A] \ \xrightarrow{\sim} \ S\,[t \mid A]_S \ : \ t^\alpha \mapsto 1_S \otimes t^\alpha$$

It remains to prove that Φ already is an isomorphism of S-algebras, so we have to verify its multiplicativity. Due to the S-linearity it suffices to check this for baisis elements. So compute

$$\Phi(t^\alpha t^\beta) = \Phi(t^{\alpha+\beta}) = 1_S \otimes t^{\alpha+\beta} = 1_S \otimes (t^\alpha t^\beta) = (1_S \otimes t^\alpha) \cdot (1_S \otimes t^\beta)$$

Matrices: Let us abbreviate $M := \mathrm{mat}_{m,n}(R)$ and $N := \mathrm{mat}_{m,n}(S)$. Then the R-module M has the Euclidean basis $\{ E_{i,j}(R) \mid i \in 1 \ldots m, j \in 1 \ldots n \}$ of elementary matrices $E_{i,j}(R)$. That is the (i,j)-th entry of $E_{i,j}(R)$ is 1_R all others are zero. Likewise N has the basis $\{ E_{i,j}(S) \mid i \in 1 \ldots m, j \in 1 \ldots n \}$ only that the (i,j)-th entry of $E_{i,j}(S)$ is 1_S. Now regard the canonical map

$$\iota \ : \ M \to N \ : \ (a_{i,j}) \mapsto (a_{i,j} 1_S)$$

Beware that ι need *not* be injective. Nevertheless, according to (3.160.(v)), we obtain a well-defined map $\iota_{(S)}$, which is defined by linear expansion of

$$\iota_{(S)} \ : \ M_S \to N \ : \ s \otimes A \mapsto s\iota(A)$$

And from this we clearly see that $\iota_{(S)}(1_S \otimes E_{i,j}(R)) = E_{i,j}(S)$. But by (3.160.(i)) M_S has the S-basis $\{ 1_S \otimes E_{i,j}(R) \mid i \in 1 \ldots m, j \in 1 \ldots n \}$. So $\iota_{(S)}$ matches the S-bases of M_S and N and hence is bijective and S-linear. But according to (3.160.(vi)) $\iota_{(S)}$ even is a homomorphism of S-algebras. In short: $\iota_{(S)}$ is the isomorphism we sought. □

Proof of (3.162):

Let us abbreviate $H_R := \mathrm{mhom}_R(M,N)$ and $H_S := \mathrm{mhom}_S(M_S,N_S)$. Clearly $S \times H_R \to H_S : (s,\varphi) \mapsto s\varphi_S$ is R-bilinear and hence induces the R-module-homomorphism $\mu : S \otimes H_R \to H_S$ by linear expansion of $\mu : s \otimes \varphi \mapsto s\varphi_S$. This map obviously not only is R-linear, but S-linear, as well. So it remains to verify the properties of this map given in the claim:

(i) If S is free with basis $\{ s_i \mid i \in I \}$ then according to (3.146.(iv)) we find the an isomorphy of R-modules $\Phi_M : M^{\oplus I} \xrightarrow{\sim} M_S$. And likewise we find $\Phi_N : N^{\oplus I} \xrightarrow{\sim} N_S$ and also

$$\Phi_H \ : \ H_R^{\oplus I} \ \xrightarrow{\sim} \ \big(H_R\big)_S \ : \ (\varphi_i) \mapsto \sum_{i\in I} s_i \otimes \varphi_i$$

On the other hand composing the isomorphy $H_S \xrightarrow{\sim} \mathrm{mhom}_R(M,N_S)$ that has been estabilshed in (3.160.(v)) $\psi \mapsto (x \mapsto \psi(1_S \otimes x))$ with the isomorphy $\Phi_N : N^{\oplus I} \xrightarrow{\sim} N_S$ we end up with the following isomorphy of R-modules

$$H_S \ \xrightarrow{\sim} \ \mathrm{mhom}_R(M,N^{\oplus I}) \ : \ \psi \mapsto \big(x \mapsto \Phi_N^{-1}\psi(1_S \otimes x)\big)$$

Now regard the map $\kappa : H_R^{\oplus I} \hookrightarrow \mathrm{mhom}_R(M,N^{\oplus I})$ which is defined by $(\varphi_i) \mapsto (x \mapsto (\varphi_i(x)))$. This map obviously is injective such that we end up with the following diagram

$$\begin{array}{ccc} \big(\mathrm{mhom}_R(M,N)\big)_S & \xrightarrow{\mu} & \mathrm{mhom}_S(M_S,N_S) \\ \updownarrow & & \updownarrow \\ \updownarrow & & \mathrm{mhom}_R(M,N_S) \\ \updownarrow & & \updownarrow \\ \mathrm{mhom}_R(M,N)^{\oplus I} & \xrightarrow{\kappa} & \mathrm{mhom}_R(M,N^{\oplus I}) \end{array}$$

It remains to prove that this diagram is truly commutative, then the injectivity of κ is transfered to ι. So let us start with some family $(\varphi_i) \in \mathrm{mhom}_R(M,N)^{\oplus I}$. Under κ this is transferred to $x \mapsto (\varphi_i(x))$ And $\Phi_N : N^{\oplus I} \to N_S$ drops it on

$$\left(x \mapsto \sum_{i\in I} s_i \otimes \varphi_i(x) \right) \ \in \ \mathrm{mhom}_R(M,N_S)$$

On the other hand (φ_i) is transferred upward to $\varphi = \sum_i s_i \otimes \varphi_i$ under Φ_H. From there μ transfers it to $\psi = \sum_i s_i(\varphi_i)_S$. Note that

$$\begin{aligned} \psi(1_S \otimes x) &= \sum_{i\in I} s_i(\varphi_i)_S(1_S \otimes x) \\ &= \sum_{i\in I} s_i(1_S \otimes \varphi_i(x)) \ = \ \sum_{i\in I} s_i \otimes \varphi_i(x) \end{aligned}$$

Now ψ is transported down to $\mathrm{mhom}_R(M,N_S)$ where it is turned into $x \mapsto \psi(1_S \otimes x) = \sum_i s_i \otimes \varphi_i(x)$. Thus the upper way delivers (φ_i) to exactly the same element of $\mathrm{mhom}_R(M,N_S)$ as the lower way. That is the diagram truly is commutative.

(ii) We continue with (i) but now have that I is finite. In this case the injective map κ even is bijective, according to (3.37) such that μ is bijective, as well.

(iii) Let $\{ m_j \mid j \in 1 \dots n \}$ be an R-basis of M, being an R-basis means that the map $\Phi_M : R^n \to M : (a_j) \mapsto \sum_j a_j m_j$ is an isomorphism of R-modules. Likewise if $\{ n_i \mid i \in 1 \dots m \}$ is an R-basis of N, then $\Phi_N : R^m \to N : (b_i) \mapsto \sum_i b_i n_i$ is an isomorphism as well. We now use the isomorphy of the R-module of module-homomorphisms with the R-module of $(n \times m)$-matrices over R, which is given to be

$$\chi \ : \ \mathrm{mat}_{n,m}(R) \ \xrightarrow{\sim} \ \mathrm{mhom}_R(M,N) \ : \ A \mapsto (x \mapsto \Phi_N A \Phi_M^{-1})$$

Then $\chi_S = S \otimes \chi : (\mathrm{mat}_{n,m}(R))_S \xrightarrow{\sim} (\mathrm{mhom}_R(M,N))_S$ is an isomorphism of R-modules, according to (3.149.(iii)). But as (by definition) $\chi_S : s \otimes A \mapsto s \otimes \chi(A)$ it is clear, that this map also is S-linear. But from example (3.159) we know that $(\mathrm{mat}_{n,m}(R))_S$ is isomorphic (as an S-module) to $\mathrm{mat}_{n,m}(S)$ under the isomorphism $s \otimes A \mapsto sA$. And using the same reasoning as for the homomorphisms $M \to N$ we find that $\mathrm{mat}_{n,m}(S) \xrightarrow{\sim} \mathrm{mhom}_S(M_S, N_S)$ where we use the induced bases $\{ 1_S \otimes m_j \mid j \in 1 \dots n \}$ and $\{ 1_S \otimes n_i \mid i \in 1 \dots m \}$ again. Putting all these together we have finally arrived at the isomorphy

$$\big(\mathrm{mhom}_R(M,N)\big)_S \ \xrightarrow{\sim} \ \mathrm{mhom}_S(M_S, M_S)$$

Let us regard how this isomorphy works: if we start with some $s \in S$ and some homomorphism $\varphi : M \to N$ then χ_S^{-1} maps $s \otimes \varphi$ to $s \otimes A$ where A is the matrix of φ that is $\chi(A) = \varphi$. This is then taken to the matrix sA which represents the homomorphism $s\varphi_S : M_S \to N_S$ by (3.160.(ii)). So altogether we have verified that truly $s \otimes \varphi \mapsto s\varphi_S$ as has been claimed.

□

Proof of (3.155):

(i) If M and N are finitely generated, say $M = \mathrm{Lh}\{ x_i \mid i \in 1 \dots m \}$ and $N = \mathrm{Lh}\{ y_j \mid j \in 1 \dots n \}$, then any $x \in M$ and any $y \in N$ can be written in the form $x = \sum_i a_i x_i$ and $y = \sum_j b_j y_j$ respectively. But this means, that the tensor $x \otimes y$ can be written as

$$x \otimes y \ = \ \sum_{i=1}^{m} \sum_{j=1}^{n} a_i b_j \, x_i \otimes y_j$$

That is any pure tensor $x \otimes y$ can be generated by the mn (finitely many) elements $\{ x_i \otimes y_j \mid i \in 1 \dots m, \ j \in 1 \dots$ And as any $t \in M \otimes M$ is a sum of pure tensors, this means that any t can be generated over these mn elements. In particular $M \otimes N$ is finitely generated.

(i) Let $\star$ abbreviate one of the words *noetherian* or *artinian*. As M is finitely generated there is a surjective homomorphism $\mu : R^m \twoheadrightarrow M$: Pick up a generating set $\{ x_i \mid i \in 1 \dots m \}$ of M then μ can be given explicitly to be $\mu(a_1, \dots, a_m) = \sum_i a_i x_i$. But according to (3.149.(iii)) we thereby find that $\mu \otimes N : R^m \otimes N \twoheadrightarrow M \otimes N$ is another surjective homomorphism of R-modules.

On the other hand proposition (3.146.(v)) tells us that there is an isomorphy $R^m \otimes N \ \cong_{\mathrm{m}} \ N^m$. Thereby N^m is a $\star$ module, since N is $\star$ and hence is its power, due to (3.111.(iv)) This of course means, that $R^m \otimes N$ is a $\star$ module again.

But since $M \otimes N = \mathrm{im}(\mu \otimes N)$ is the image of the $\star$ module $R^m \otimes N$ under the surjective homomprphism $\mu \otimes N$ theorem (3.111.(v)) finally tells us, that $M \otimes N$ is $\star$. as well.

(ii) If M and N are finitely generated, then so is $M \otimes N$, according to (i). And if M and N are free, then so is $M \otimes N$ according to (3.146.(vi)). Now if M and N are noetherian, then in particular M is finitely generated. Hence $M \otimes N$ is noetherian, according to (i) again. If M and N are artinian, then $M \otimes N$ is a module of finite length, as we have seen in (3.120) and in particular $M \otimes N$ is an artinian module again, due to (3.119.(vi)).

(iii) If both M and N are of finite length, then let us regard a composition series of M, that is $0 = M_0 \subset M_1 \subset M_2 \subset \ldots \subset M_p = M$ where $p = \ell(M)$ and any M_k/M_{k-1} is a simple R-module. That is there are some $m_i \in M$ such that $M_i = M_{i-1} + Rm_i$ and in particular M is finitely generated by the elements $\{ m_1, \ldots, m_p \}$.

Thus we find a surjective map $\mu : R^p \twoheadrightarrow M : (a_1, \ldots, a_p) \mapsto \sum_i a_i m_i$. Tensoring this with N we maintain the surjectivity of the homomorphism $\mu \otimes N : R^p \otimes N \twoheadrightarrow M \otimes N$. And thereby $N^p \cong_{\mathfrak{m}} R^p \otimes N$ are isomorphic by (3.146.(v)) again.

According to the Jordan-Hölder theorem (check the remark following it) N^p has finite length $\ell(N^p) = \ell(N^{\oplus p}) = p \cdot \ell(N) = \ell(M) \cdot \ell(N)$. And as $\mu \otimes N$ is surjective and $R^p \otimes N$ has finite length, so does $M \otimes N$. To be precise we find the claim

$$\ell(M \otimes N) \;\leq\; \ell(R^p \otimes N) \;=\; \ell(N^p) \;=\; \ell(M) \cdot \ell(N)$$

(iv) Pick up any R-module N and denote the R-module of R-linear maps from $M \to N$ by $H := \mathcal{L}(M, N)$. Then by assumption and (3.93) we find the following exact chain of R-modules

$$0 \to \mathcal{L}(W, H) \xrightarrow{\psi^*} \mathcal{L}(V, H) \xrightarrow{\varphi^*} \mathcal{L}(U, H)$$

Recall that $H = \mathcal{L}(M, N)$ is another module of homomorphisms and hence we have the isomorphy $\mathcal{L}(W \otimes M, N) \xrightarrow{\sim} \mathcal{L}(W, H) : \gamma \mapsto \gamma'$ where $\gamma'(w)(m) = \beta(w \otimes m)$ according to (the remark following) (3.142). That is we have arrived at the following diagram of R-module homomorphisms [where we abbreviated $W_M := W \otimes M$ and $\psi_M := \psi \otimes \mathbb{1}_M$ and so on for notational reasons. The vertical homomorphisms are the isomorphies $\sigma \mapsto \gamma'$ and $\beta \mapsto \beta'$ respectively]

$$\begin{array}{ccccccc}
0 & \to & \mathcal{L}(W, H) & \xrightarrow{\psi^*} & \mathcal{L}(V, H) & \xrightarrow{\varphi^*} & \mathcal{L}(U, H) \\
 & & \updownarrow & & \updownarrow & & \updownarrow \\
0 & \to & \mathcal{L}(W_M, N) & \xrightarrow{\psi_M^*} & \mathcal{L}(V_M, N) & \xrightarrow{\varphi_M^*} & \mathcal{L}(U_M, N)
\end{array}$$

Next we will prove that this diagram commutes: Let us start with $\gamma \in \mathcal{L}(W \otimes M, N)$. On the bottom line we get for any $v \in V$ and any $m \in N$ that $(\psi \otimes M)^*(\gamma)(v \otimes m) = \gamma \circ (\psi \otimes M)(v \otimes m) = \gamma(\psi(v) \otimes m)$. But this is precisely the same, as $(\psi^*(\gamma'))(v)(m) = ((\gamma'\psi)(v))(m) = \gamma'(\psi(v))(m) = \gamma(\psi(v) \otimes m)$. In complete analogy we see the commutativity of the second (left) square, if we start with some $\beta \in \mathcal{L}(V \otimes M, N)$.

Due to the commutativity of the diagram the bottom line inherits the exactness form the top line, according to (3.92). But as the module N can be chosen arbitrarily the lemma of Yoneda (3.94.(ii))

tells us that the following chain of R-modules truly is exact, as claimed

$$U \otimes M \overset{\varphi \otimes M}{\longrightarrow} V \otimes M \overset{\psi \otimes M}{\longrightarrow} W \otimes M \to 0$$

(v) The inclusion $\mathrm{im}(\varphi_1 \otimes N_1) + \mathrm{im}(M_1 \otimes \psi_1) \subseteq \mathrm{kn}(\varphi_2 \otimes \psi_2)$ is easy to see: due to the composition properties of the tensor product of maps we have

$$(\varphi_2 \otimes \psi_2)(\varphi_1 \otimes N_1) \;=\; \varphi_2\varphi_1 \otimes \varphi_1 \;=\; 0 \otimes \varphi_1 \;=\; 0$$

such that $\mathrm{im}(\varphi_1 \otimes N_1) \subseteq \mathrm{kn}(\varphi_2 \otimes \psi_2)$. Likewise we find $\mathrm{im}(M_1 \otimes \psi_1) \subseteq \mathrm{kn}(\varphi_2 \otimes \psi_2)$ and hence the sum is contained in the kernel, as well.

For the converse inclusion $\mathrm{kn}(\varphi_2 \otimes \psi_2) \subseteq \mathrm{im}(\varphi_1 \otimes N_1) + \mathrm{im}(M_1 \otimes \psi_1)$ we note in advance that according to (iv) for any $k \in 0 \ldots 2$ the following chain of R-modules is exact

$$M_0 \otimes N_k \overset{\varphi_1 \otimes N_k}{\longrightarrow} M_1 \otimes N_k \overset{\varphi_2 \otimes N_k}{\longrightarrow} M_2 \otimes N_k \to 0$$

and in particular $\mathrm{kn}(\varphi_2 \otimes N_k) = \mathrm{im}(\varphi_1 \otimes N_k)$. Likewise it is clear, that for any $i \in 0 \ldots 2$ we also have $\mathrm{kn}(M_i \otimes \psi_2) = \mathrm{im}(M_i \otimes \psi_1)$. We will use these equalities several times.

Now consider any $t \in \mathrm{kn}(\varphi_2 \otimes \psi_2) \subseteq M_1 \otimes N_1$, then we need to prove $t \in \mathrm{im}(\varphi_1 \otimes N_1) + \mathrm{im}(M_1 \otimes \psi_1)$. But first of all we may compute

$$0 \;=\; (\varphi_2 \otimes \psi_2)(t) \;=\; (\varphi_2 \otimes N_2)(M_1 \otimes \psi_2)(t)$$

and hence we find $(M_1 \otimes \psi_2)(t) \in \mathrm{kn}(\varphi_2 \otimes N_2) = \mathrm{im}(\varphi_1 \otimes N_2)$. That is there is some $q \in M_0 \otimes N_2$ such that

$$(\varphi_1 \otimes N_2)(q) \;=\; (M_1 \otimes \psi_2)(t)$$

Also, as ψ_2 is surjective, so is $M_0 \otimes \psi_2 : M_0 \otimes N_1 \to M_0 \otimes N_2$ and hence there is some $p \in M_0 \otimes N_1$ such that $q = (M_0 \otimes \psi_2)(p)$. Now $(\varphi_1 \otimes \psi_2)(p) = (\varphi_1 \otimes N_2)(M_0 \otimes \psi_2)(p) = (\varphi_1 \otimes N_2)(q) = (M_1 \otimes \psi_2)(t)$ or equivalently

$$\begin{aligned} 0 &= (M_1 \otimes \psi_2)(t) - (\varphi_1 \otimes \psi_2)(p) \\ &= (M_1 \otimes \psi_2)(t) - (M_1 \otimes \psi_2)(\varphi_1 \otimes N_1)(p) \\ &= (M_1 \otimes \psi_2)\Big(t - (\varphi_1 \otimes N_1)(p)\Big) \end{aligned}$$

This implies $t - (\varphi_1 \otimes N_1)(p) \in \mathrm{kn}(M_1 \otimes \psi_2) = \mathrm{im}(M_1 \otimes \psi_1)$. That is there is some $p' \in M_1 \otimes N_0$ such that $t - (\varphi_1 \otimes N_1)(p) \;=\; (M_1 \otimes \psi_1)(p')$. So altogether we found

$$t \;=\; (\varphi_1 \otimes N_1)(p) + (M_1 \otimes \psi_1)(p') \;\in\; \mathrm{im}(\varphi_1 \otimes N_1) + \mathrm{im}(M_1 \otimes \psi_1)$$

(ii) Now assume that both M an N have a finite free presentation, that is there are exect chains of R-modules of the following form

$$R^p \;\overset{\varphi}{\longrightarrow}\; R^m \;\overset{\mu}{\longrightarrow}\; M \;\to\; 0$$

$$R^q \xrightarrow{\varphi} R^n \xrightarrow{\nu} N \to 0$$

Since both μ and ν are surjective, so is $\mu \otimes \nu$ and hence we find the following exact chain of R-modules

$$R^m \otimes R^n \xrightarrow{\mu \otimes \nu} M \otimes N \to 0$$

Note that $R^m \otimes R^n$ is isomorphic to R^{mn} and hence we already have a candidate for the end of our finite free presentation of $M \otimes N$. Also by (v) we explicitly know the kernel of $\mu \otimes \nu$ to be

$$\mathrm{kn}(\mu \otimes \nu) = \mathrm{im}(\varphi \otimes R^n) + \mathrm{im}(R^m \otimes \psi)$$

In particular we see, that the kernel is finitely generated again: Let e_1 to e_p be a basis of R^p and f_1 to f_q be a basis of R^q. Then we see that the kernel of $\mu \otimes \nu$ is precisely given to be the linear hull of

$$\begin{aligned} \mathrm{kn}(\mu \otimes \nu) &= \mathrm{Lh}\{\, \varphi(e_i) \otimes f_k \mid i \in 1 \ldots p,\, k \in 1 \ldots q \,\} \\ &\quad + \mathrm{Lh}\{\, e_j \otimes \psi(f_\ell) \mid j \in 1 \ldots p,\, \ell \in 1 \ldots q \,\} \end{aligned}$$

Hence we let $N := p \cdot n + m \cdot q$ and take $\kappa : R^N \to R^m \otimes R^n$ to be the R-linear map that gives a linear expansion of these generators

$$\kappa(a_{i,k}, b_{j,\ell}) := \sum_{i=1}^{p} \sum_{k=1}^{q} a_{i,k}\, \varphi(e_i) \otimes f_k + \sum_{j=1}^{p} \sum_{\ell=1}^{q} b_{j,\ell}\, e_j \otimes \psi(f_\ell)$$

then by construction the image of κ is precisely the kernel of $\mu \otimes \nu$. And thereby we have found a finite free presentation of $M \otimes N$

$$R^N \xrightarrow{\kappa} R^m \otimes R^n \xrightarrow{\mu \otimes \nu} M \to 0$$

□

Proof of (3.153):
If the m_i and n_j satisfy these properties, it is easy to compute, that their tensor product truly vanishes

$$\begin{aligned} \sum_{j \in J} m_j \otimes n_j &= \sum_{j \in J} \left(\sum_{i=1}^{m} a_{i,j} x_j \right) \otimes n_j = \sum_{j \in J} \sum_{i=1}^{m} a_{i,j} x_j \otimes n_j \\ &= \sum_{i=1}^{m} x_j \otimes \left(\sum_{j \in J} a_{i,j} n_j \right) = \sum_{i=1}^{m} x_j \otimes 0 = 0 \end{aligned}$$

Conversely we assume the tensor to be zero and want to show that all these $x_i \in M$ and $a_{i,j} \in R$ exist and satisfy the properties required of them. Since $\{\, n_j \mid j \in J \,\}$ generates N the map $\nu : R^{\oplus J} \to N$ defined by $\nu(b) = \sum_j b_j n_j$ is surjective. Hence we get a short exact chain of R-modules

$$0 \to \mathrm{kn}(\nu) \xrightarrow{\subseteq} R^{\oplus J} \xrightarrow{\nu} N \to 0$$

And according to (3.155.(iv)) we thereby get another exact chain of R-modules by tensoring with M

$$M \otimes \mathrm{kn}(\nu) \overset{M\otimes \subseteq}{\longrightarrow} M \otimes R^{\oplus J} \overset{M\otimes \nu}{\longrightarrow} M \otimes N \to 0$$

Let $\left\{ e_j \mid j \in J \right\}$ be the standard Euclidean basis of $R^{\oplus J}$ then $\nu(e_j) = n_j$ and hence we find $(M \otimes \nu)(\sum_j m_j \otimes e_j) = \sum_j m_j \otimes n_j = 0$ by assumption, such that $\sum_j m_j \otimes e_j \in \mathrm{kn}(M \otimes \nu) = \mathrm{im}(M\otimes \subseteq)$. That is there is some $\sum_i x_i \otimes k_i \in M \otimes \mathrm{kn}(\nu)$ such that

$$\sum_{i=1}^{m} x_i \otimes k_i \;=\; (M\otimes \subseteq) \left(\sum_{i=1}^{m} x_i \otimes k_i \right) \;=\; \sum_{j\in J} m_j \otimes e_j$$

Now write $k_i \in \mathrm{kn}(\nu) \subseteq R^{\oplus J}$ as $k_i = \sum_j a_{i,j} e_j$ [which is possible, as the e_j form a basis of $R^{\oplus J}$], then clearly

$$0 \;=\; \nu(k_i) \;=\; \sum_{j\in J} a_{i,j} \nu(e_j) \;=\; \sum_{j\in J} a_{i,j} n_j$$

for any $i \in 1 \ldots m$ and this already is the first property. For the second property we compute

$$\begin{aligned} \sum_{j\in J} m_j \otimes e_j \;&=\; \sum_{i=1}^{m} x_i \otimes k_i \;=\; \sum_{i=1}^{m} x_i \otimes \left(\sum_{j\in J} a_{i,j} e_j \right) \\ &=\; \sum_{j\in J} \left(\sum_{i=1}^{m} a_{i,j} x_i \right) \otimes e_j \end{aligned}$$

Recall that by (3.146.(v)) we have the isomorphy $M^{\oplus J} \overset{\sim}{\longrightarrow} M \otimes R^{\oplus J}$ given by $(m_j) \mapsto \sum_j m_j \otimes e_j$. That is the above sums are identical images under this isomorphism and hence their preimages are equal as well. This is the second property - for any $j \in J$ we get

$$m_j \;=\; \sum_{i=1}^{m} a_{i,j} x_i$$

□

Proof of (3.139):

(i) By definition the support of M is empty iff we have $M_\mathfrak{p} = 0$ for any $\mathfrak{p} \in \mathrm{Spec}(R)$. So this is property (b) in (3.135). So the claim is just a reformulation of (a) $\iff$ (b) in said proposition.

(ii) Let $P := 0$, then for any $\mathfrak{p} \in \mathrm{Spec}(R)$ we clearly have $P_\mathfrak{p} = 0$, as well. So by (3.136) we have the equivalence of

$$x = 0 \quad\iff\quad \forall\, \mathfrak{m} \in \mathrm{Smax}(R) \,:\, \frac{x}{1} = \frac{0}{1}$$

for any $x \in M$. As $\mathrm{Smax}(R) \subseteq \mathrm{Spec}(R)$ we get the same equivalence with the prime instead od the maximal spectrum. But if $\mathfrak{p} \in \mathrm{Spec}(R)$ is prime, but $\mathfrak{p} \notin \mathrm{Supp}(M)$, then $P_\mathfrak{p} \subseteq M_\mathfrak{p} = 0$ such that $x/1 = 0/1$ anyhow. That is these $\mathfrak{p}$ do not contribute to the truth of the statement and hence

$$x = 0 \quad\iff\quad \forall\, \mathfrak{p} \in \mathrm{Supp}(R) \,:\, \frac{x}{1} = \frac{0}{1}$$

But this is the (well-definedness) and injectivity of the endomorphism given in the claim. And the

homomorphism property is trivial.

(iii) Consider some $\mathfrak{p} \notin \mathbb{V}(\mathfrak{a})$, that is there is some $a \in \mathfrak{a}$ such that $a \notin \mathfrak{p}$. That is $a \in U := R \setminus \mathfrak{p}$ is contained in the multiplicatively closed set of the localization. Thus for any $(b+\mathfrak{a})/u \in (R/\mathfrak{a})_\mathfrak{p}$ we have

$$a\frac{b+\mathfrak{a}}{u} \;=\; \frac{ab+\mathfrak{a}}{u} \;=\; \frac{0+\mathfrak{a}}{u} \;=\; a\frac{0+\mathfrak{a}}{1} \;=\; 0$$

That is for any $x = (b+\mathfrak{a})/u \in (R/\mathfrak{a})_\mathfrak{p}$ there is $a \in U$ such that $ax = 0$ and hence $(R/\mathfrak{a})_\mathfrak{p} = 0$. This means $\mathfrak{p} \notin \operatorname{Supp}(R/\mathfrak{a})$, as well.

Conversely, if $\mathfrak{p} \in \mathbb{V}(\mathfrak{a})$ then $\mathfrak{a} \subseteq \mathfrak{p}$ and thereby $\mathfrak{a}_\mathfrak{p} := U^{-1}\mathfrak{a} \subseteq \mathfrak{m}_\mathfrak{p} := U^{-1}\mathfrak{p}$. Note that $\mathfrak{m}_\mathfrak{p}$ is *the* maximal ideal of $R_\mathfrak{p}$. But by (2.132.(vi)) we also have an isomorphy of the form

$$\Big(R\Big/\mathfrak{a}\Big)_\mathfrak{p} \;\cong_\mathsf{r}\; R_\mathfrak{p}\Big/\mathfrak{a}_\mathfrak{p} \;\neq\; 0$$

In particular $(R/\mathfrak{a})_\mathfrak{p} \neq 0$ which means $\mathfrak{p} \in \operatorname{Supp}(R/\mathfrak{a})$. Together this is the equality of the subsets $\mathbb{V}(\mathfrak{a}) = \operatorname{Supp}(R/\mathfrak{a})$ of the spectrum of R.

(iv) We start with the general statement: Given a short exact chain $0 \to L \to M \to N \to 0$ of R-modules, where $\varphi : L \to M$ and $\psi : M \to N$ are the respective homomorphisms, any prime ideal $\mathfrak{p} \trianglelefteq_\mathsf{i} R$ gives rise to another short exact chain of R-modles, according to (3.126)

$$0 \;\to\; L_\mathfrak{p} \;\to\; M_\mathfrak{p} \;\to\; N_\mathfrak{p} \;\to\; 0$$

If $\mathfrak{p} \notin \operatorname{Supp}(M)$ then $M_\mathfrak{p} = 0$. As $L_\mathfrak{p} \hookrightarrow M_\mathfrak{p}$ is injective this implies $L_\mathfrak{p} = 0$ and as $M_\mathfrak{p} \twoheadrightarrow N_\mathfrak{p}$ is surjective this implies $N_\mathfrak{p} = 0$ such that $\mathfrak{p} \notin \operatorname{Supp}(L)$ and $\mathfrak{p} \notin \operatorname{Supp}(N)$. If we abbreviate $\mathcal{S} := \operatorname{Spec}(R)$ that is the inclusion

$$\mathcal{S} \setminus \operatorname{Supp}(M) \;\subseteq\; \big(\mathcal{S} \setminus \operatorname{Supp}(L)\big) \cap \big(\mathcal{S} \setminus \operatorname{Supp}(N)\big)$$

But the converse inclusion is true as well: If *both* $L_\mathfrak{p} = 0$ and $N_\mathfrak{p} = 0$ then $0 \hookrightarrow M_\mathfrak{p} \twoheadrightarrow 0$. And as $M_\mathfrak{p} = \ker(\psi_\mathfrak{p}) = \operatorname{im}(\varphi_\mathfrak{p}) = 0$ we also have $M_\mathfrak{p} = 0$ such that $\mathfrak{p} \notin \operatorname{Supp}(M)$. Now by going to complements we find the claim from the equation

$$\mathcal{S} \setminus \operatorname{Supp}(M) \;=\; \big(\mathcal{S} \setminus \operatorname{Supp}(L)\big) \cap \big(\mathcal{S} \setminus \operatorname{Supp}(N)\big) \;=\; \mathcal{S} \setminus \big(\operatorname{Supp}(L) \cup \operatorname{Supp}(N)\big)$$

Now return to the case $L = P \leq_\mathsf{m} M$ and $N = M/P$. It suffices to present the following short exact chain of R-modules: Let $\varphi := \iota : P \hookrightarrow M : x \mapsto x$ and $\psi := \varrho : M \twoheadrightarrow M/P : x \mapsto x + P$, then $\operatorname{Supp}(M)$ is the union of $\operatorname{Supp}(P)$ and $\operatorname{Supp}(M/P)$, as these give rise to the chain

$$0 \;\to\; P \;\to\; M \;\to\; M\Big/P \;\to\; 0$$

(v) Let us abbreviate $\mathcal{S} := \operatorname{Spec}(R)$ and $P := \sum_i P_i$ and consider some prime ideal $\mathfrak{p} \trianglelefteq_\mathsf{i} R$ such that $P_\mathfrak{p} = 0$. That is for any $x \in P$ there is some $u \in U := R \setminus \mathfrak{p}$ such that $ux = 0$. As any $P_i \subseteq P$ this means that $(P_i)_\mathfrak{p} = 0$, too and thereby

$$\mathcal{S} \setminus \operatorname{Supp}(P) \;\subseteq\; \mathcal{S} \setminus \operatorname{Supp}(P_i)$$

By going to complements this is $\mathrm{Supp}(P_i) \subseteq \mathrm{Supp}(P)$ for any $i \in I$. Conversely suppose $(P_i)_\mathfrak{p} = 0$ for any $i \in I$ and pick up some $x \in P$. That is there is a finite subset $\Omega \subseteq I$ and some $x_i \in P_i$ (where $i \in \Omega$) such that $x = \sum_i x_i$ (where the sum runs over $i \in \Omega$). As $(P_i)_\mathfrak{p} = 0$ there is some $u_i \in U$ such that $u_i x_i = 0$. Now let $u := \prod u_i$ (where the product runs over $i \in \Omega$), as U is multiplicatively closed we have $u \in U$ and $ux = \sum_i ux_i = \sum_i 0 = 0$ is clear. Therefore we also have the inclusion

$$\mathcal{S} \setminus \bigcup_{i\in I} \mathrm{Supp}(P_i) \;=\; \bigcap_{i\in I} \mathcal{S} \setminus \mathrm{Supp}(P_i) \;\subseteq\; \mathcal{S} \setminus \mathrm{Supp}(P)$$

By going to complements again, we also find $\bigcup_i \mathrm{Supp}(P_i) \subseteq \mathrm{Supp}(P)$, such that we have established the desired identity.

(viii) In a first step let us prove the claim for finitely generated modules M and N over a local ring S with maximal ideal $\mathfrak{m}$. Let $E := S/\mathfrak{m}$ be the quotient field of S and $M_E := E \otimes_S M$ and likewise $N_E := E \otimes_S N$. We know by (3.159) that M_E is isomorphic to $M_E \xrightarrow{\sim} M/\mathfrak{m}M$. And thereby the lemma of Nakayama (3.44.(ii)) [note that $\mathfrak{m} = \mathrm{JAC}(S)$] implies the equivalence of

$$M_E = 0 \iff M = \mathfrak{m}M \iff M = 0$$

As M_E is an E-module and E is a field, M_E is free, likewise N_E. Also by (3.160.(v)) we have an isomorphy of E-modules of the form

$$\big(M \otimes_S N\big)_E \xrightarrow{\sim} M_E \otimes_E N_E$$

In particular these modules share the same dimension. But as M_E and N_E are free (3.146.(vi)) implies the equality of the dimension

$$\dim\Big(\big(M \otimes_S N\big)_E\Big) \;=\; \dim\big(M_E \otimes_E N_E\big) \;=\; \dim\big(M_E\big) \cdot \dim\big(N_E\big)$$

That is $(M \otimes_S N)_E = 0$ is equivalent to $M_E = 0$ or $N_E = 0$. But we have already argued, that these statements are equivalent to

$$M \otimes_S N = 0 \iff M = 0 \quad \text{or} \quad N = 0$$

Let us now consider finitely generated modules M and N over an arbitrary commutative ring R. Then we would like to show the equality of the support

$$\mathrm{Supp}(M \otimes N) \;=\; \mathrm{Supp}(M) \cap \mathrm{Supp}(N)$$

So consider any prime ideal $\mathfrak{p} \trianglelefteq_\mathrm{i} R$ and let $S := R_\mathfrak{p}$ then S is a local ring with maximal ideal $\mathfrak{p}S$. And $\mathfrak{p} \notin \mathrm{Supp}(M \otimes_R N)$ iff $(M \otimes_R N)_\mathfrak{p} = 0$. But by (3.151) we have the isomorphies

$$\big(M \otimes_R N\big)_\mathfrak{p} \;\cong_\mathfrak{m}\; M_\mathfrak{p} \otimes_R N_\mathfrak{p} \;\cong_\mathfrak{m}\; \big(M_\mathfrak{p} \otimes_S N_\mathfrak{p}\big)_R$$

Hence $M \otimes_R N = 0$ is equivalent to $M_\mathfrak{p} \otimes_S N_\mathfrak{p} = 0$. But as S is a local ring, we have already argued that this again is equivalent to $M_\mathfrak{p} = 0$ or $N_\mathfrak{p} = 0$. But this is $\mathfrak{p} \notin \mathrm{Supp}(M)$ or $\mathfrak{p} \notin \mathrm{Supp}(N)$.

Negating this we find the desired equivalence

$$\mathfrak{p} \in \operatorname{Supp}(M \otimes_R N) \iff \mathfrak{p} \in \operatorname{Supp}(M) \text{ and } \mathfrak{p} \in \operatorname{Supp}(N)$$

(vi) For any $i \in I$ we have $R/\mathfrak{a}_i \xrightarrow{\sim} Rm_i : a + \mathfrak{a}_i \mapsto am_i$ according to (3.22.(ii)). Thereby $\operatorname{Supp}(Rm_i) = \operatorname{Supp}(R/\mathfrak{a}_i) = \mathbb{V}(\mathfrak{a}_i)$ due to (iii). If now $M = \operatorname{Lh}\{ m_i \mid i \in I \}$ then $M = \sum_i Rm_i$ so by (iv) we get

$$\operatorname{Supp}(M) = \bigcup_{i\in I} \operatorname{Supp}(Rm_i) = \bigcup_{i\in I} \mathbb{V}(\mathfrak{a}_i)$$

If M is finitely generated, say $I = 1 \dots n$ then $\mathfrak{a} := \operatorname{ann}(M) = \bigcap_i \mathfrak{a}_i$ and as I is finite (2.16) implies

$$\operatorname{Supp}(M) = \bigcup_{i=1}^{n} \mathbb{V}(\mathfrak{a}_i) = \mathbb{V}\left(\bigcap_{i=1}^{n} \mathfrak{a}_i\right) = \mathbb{V}(\mathfrak{a})$$

Now suppose that $\mathfrak{a} \trianglelefteq_{\mathsf{i}} R$ is an ideal of R, then by (3.146.(ii)) we have the isomorphy $(R/\mathfrak{a}) \otimes M \cong_{\mathsf{m}} M/\mathfrak{a}M$. In particular we may invoke (viii), (iii) and (2.16) to find its support

$$\begin{aligned}
\operatorname{Supp}\left(M \Big/ \mathfrak{a}M\right) &= \operatorname{Supp}\left(R \Big/ \mathfrak{a} \otimes M\right) \\
&= \operatorname{Supp}\left(R \Big/ \mathfrak{a}\right) \cap \operatorname{Supp}(M) \\
&= \mathbb{V}(\mathfrak{a}) \cap \mathbb{V}\big(\operatorname{ann}(M)\big) \\
&= \mathbb{V}\big(\mathfrak{a} + \operatorname{ann}(M)\big)
\end{aligned}$$

(vii) As M is finitely generated, we find that the intersection of all $\mathfrak{p} \in \operatorname{Supp}(M)$ is the radical of the annihilator of M, by (vi) and (2.25.(i))

$$\bigcap \operatorname{Supp}(M) = \bigcap \mathbb{V}(\operatorname{ann}(M)) = \sqrt{\operatorname{ann}(M)}$$

Therefore $a \in \bigcap \operatorname{Supp}(M)$ is equivalent to $a^n \in \operatorname{ann}(M)$ for some $n \in \mathbb{N}$. And this again means $a^n M = 0$.

Now consider a finitely generated ideal $\mathfrak{a} \trianglelefteq_{\mathsf{i}} R$. As the grand intersection reverses the order under inclusion we find that $\mathbb{V}(\operatorname{ann}(M)) = \operatorname{Supp}(M) \subseteq \mathbb{V}(\mathfrak{a})$ is equivalent, to

$$\sqrt{\mathfrak{a}} = \bigcap \mathbb{V}(\mathfrak{a}) \subseteq \bigcap \mathbb{V}(\operatorname{ann}(M)) = \sqrt{\operatorname{ann}(M)}$$

As $\mathfrak{a}$ is finitely generated $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}} \subseteq \sqrt{\operatorname{ann}(M)}$ implies $\mathfrak{a}^n \subseteq \operatorname{ann}(M)$ for some $n \in \mathbb{N}$, according to (2.25.(vii)). And $\mathfrak{a}^n M = 0$ is just a reformulation of this. Conversely suppose $\mathfrak{a}^n \subseteq \operatorname{ann}(M)$ for some $n \in \mathbb{N}$. If $n = 0$ then $\operatorname{ann}(M) = R$ and hence $M = 0$. This would imply $\operatorname{Supp}(M) = \emptyset$ and in particular $\operatorname{Supp}(M) = \emptyset \subseteq \mathbb{V}(\mathfrak{a})$. Thus consider $n \geq 1$ then by (2.25.(vi)) we get $\sqrt{\mathfrak{a}} \subseteq \sqrt{\mathfrak{a}^n} \subseteq \sqrt{\operatorname{ann}(M)}$ and therefore $\operatorname{Supp}(M) \subseteq \mathbb{V}(\mathfrak{a})$.

(viii) It remains to prove the second part of the claim in (viii). By (i) we know that $M \otimes N = 0$ is equivalent to $\operatorname{Supp}(M \otimes N) = \emptyset$. But as $\operatorname{Supp}(M \otimes N) = \operatorname{Supp}(M) \cap \operatorname{Supp}(N)$ and the fact, that M and N are finitely generated, by assumption, we have $\operatorname{Supp}(M) = \mathbb{V}(\operatorname{ann}(M))$ and

$\mathrm{Supp}(N) = \mathbb{V}(\mathrm{ann}(N))$ according to (vi). That is

$$\mathrm{Supp}(M \otimes N) \;=\; \mathrm{Supp}(M) \cap \mathrm{Supp}(N) \;=\; \mathbb{V}(\mathrm{ann}(M)) \cap \mathbb{V}(\mathrm{ann}(N))$$

Yet by (2.32) this is $\mathrm{Supp}(M \otimes N) = \mathbb{V}(\mathrm{ann}(M) + \mathrm{ann}(N))$. As any proper ideal is contained in a maximal ideal and this is prime, we have $\mathrm{Supp}(M \otimes N) = \emptyset$ if and only if $\mathrm{ann}(M) + \mathrm{ann}(N) = R$.

□

Proof of (5.4):
By definition $M(q) = \{\, x \in M \mid \exists\, n \in \mathbb{N} : q^n x = 0 \,\}$. And by construction any element of M is of the form $x = (a_{i,j} + p(j)^{n(i,j)}R)$ for some $a_{i,j} \in R$. Thus $q^n x = 0$ is equivalent to $q^n a_{i,j} \in p(j)^{n(i,j)}R$ for any $j \in 1 \ldots s$ and any $i \in 1 \ldots I(j)$. This in turn is equivalent, to

$$q^n x \;=0 \quad\Longleftrightarrow\quad \forall\, j \in 1 \ldots s \;\; \forall\, i \in 1 \ldots I(j) \;:\; p(j)^{n(i,j)} \;\mid\; q^n a_{i,j}$$

As R is an UFD the divisibility $p(j)^{n(i,j)} \;\mid\; q^n a_{i,j}$ can be rewritten, as $\langle p \mid p(j)^{n(i,j)} \rangle \leq \langle p \mid q^n a_{i,j} \rangle$ for any prime element $p \in R$, according to (2.64.(iii)). But the only prime occurring in $p(j)^{n(i,j)}$ is $p(j)$ so this condition boils down, to

$$q^n x \;=0 \quad\Longleftrightarrow\quad \forall\, j \in 1 \ldots s \;\; \forall\, i \in 1 \ldots I(j) \;:\; n(i,j) \;\leq\; \langle q(j) \mid q^n a_{i,j} \rangle$$

We now distinguish two cases: If $q \approx p(k)$ then $n(i,k) \leq \langle q(k) \mid q^n a_{i,j} \rangle$ can easily be accomplished by taking $n := \max\{\, n(i,k) \mid i \in 1 \ldots I(k) \,\}$. If $q \approx p(j)$ is untrue, then $\langle p(j) \mid q^n \rangle = n \cdot \langle p(j) \mid q \rangle = 0$ such that by (2.64.(ii)) we get $n(i,j) \leq \langle p(j) \mid q^n a_{i,j} \rangle = \langle p(j) \mid q^n \rangle + \langle p(j) \mid a_{i,j} \rangle = \langle p(j) \mid a_{i,j} \rangle$. But this already is $a_{i,j} \in p(j)^{n(i,j)}R$ such that these $a_{i,j} + p(j)^{n(i,j)}$ have to be zero in the first place. This proved two things: (1) If $q \approx p(k)$ then $M(q)$ consists precisely of those x that can be written with $a_{i,j} = 0$ for any $j \neq k$ and (2) if $q \approx p(j)$ is untrue for all the $j \in 1 \ldots s$, then $M(q)$ only consists of $x = 0$. Both of these consequences have been formulated in the claim. □

15.6 Proofs of Chapter 5

Proof of (5.3):

(i) If $x \in L(p)$ then there is some $n \in \mathbb{N}$ such that $p^n x = 0$. In particular, as R is commutative, we find that $(ap)^n x = a^n(p^n x) = a^n\, 0 = 0$ such that $x \in L(ap)$, as well. Hence $L(p) \subseteq L(ap)$.

(ii) Clearly $0 \in L(p)$ since $p\,0 = 0$. Consider x, $y \in L(p)$ that is $p^m x = 0$ and $p^n y = 0$ for some m, $n \in \mathbb{N}$. If $a \in R$ then $p^m(ax) = a(p^m x) = a\,0 = 0$ such that $ax \in L(p)$ again. Now let $u := \max\{\, m, n \,\}$ then we also get $x + y \in L(p)$ from

$$p^u(x+y) \;=\; p^{u-m}(p^m x) + p^{u-n}(p^n y) \;=\; p^{u-m}\,0 + p^{u-n}\,0 \;=\; 0$$

(iii) First suppose that p annihilates M: As any $x \in L$ also is in $x \in M = M(p)$ there is some $n \in \mathbb{N}$ such that $p^n x = 0$. In particular we have $x \in L(p)$ again, such that p annihilates L, as well. Now consider $x + L \in M/L$, as $x \in M = M(p)$ we again find $p^n x = 0$ for some $n \in \mathbb{N}$. But thereby $p^n(x + L) = p^n x + L = 0 + L = 0 \in M/L$. And that is $x + L \in (M/L)(p)$ again.

Conversely suppose p annihilates both L and M/L and consider any $x \in M$. Then there is some $u \in \mathbb{N}$ such that $p^u(x + L) = 0 + L$ but this is nothing but $p^u x \in L$. Again, as p annihilates L, this means there is some $v \in \mathbb{N}$, such that $p^v(p^u x) = 0$. Now let $n := u + v$, then $p^n x = p^v(p^u x) = 0$ such that $x \in M(p)$. And as this is true for any $x \in M$ we have shown, that p annihilates M, too.

(iv) Consider any $x \in L_1 + \cdots + L_r$, that is x is of the form $x = x_1 + \cdots + x_r$ for some $x_i \in L_i$. As p annihilates all the L_i, there are some $n(i) \in \mathbb{N}$ such that $p^{n(i)} x_i = 0$. Now let $n := \max\{\, n(1), \ldots, n(r) \,\}$ then we easily compute

$$p^n x \;=\; \sum_{i=1}^{r} p^{n-n(i)} p^{n(i)} x_i \;=\; \sum_{i=1}^{r} p^{n-n(i)}\, 0 \;=\; 0$$

In particular we have $x \in (L_1 + \cdots + L_r)(p)$ and as x has been arbitrary this means, that p annihilates $L_1 + \cdots + L_r$ again.

(v) If $x \in M(p)$ then there is some $n \in \mathbb{N}$ such that $p^n x = 0$. In particular $0 = \varphi(p^n x) = p^n \varphi(x)$ such that $\varphi(x) \in N(p)$. And if $x \in \varphi^{-1}(N(p))$ that is $\varphi(x) \in N(p)$ there is some $n \in \mathbb{N}$ such that $0 = p^n \varphi(x) = \varphi(p^n x)$. If now φ is injective, then this implies $p^n x = 0$ such that $x \in M(p)$.

□

Proof of (5.6):

(i) Consider any $x \in R$ with $x \neq 0$. Then $\operatorname{ann}(x) = \{\, a \in R \mid ax = 0 \,\}$. But as $x \neq 0$ and R is an integral domain $ax = 0$ implies $a = 0$. Hence we get $\operatorname{ann}(x) = 0$. That is any annihilator ideal of R is 0.

Conversely: As $M \neq 0$ there there is some $x \in M \subseteq R$ with $x \neq 0$. And as we have seen, we get $\operatorname{ann}(x) = 0$ for this x, such that $0 \in \operatorname{Anns}(M)$. And as R is an integral domain $0 = \operatorname{ann}(x)$ is prime, such that $0 \in \operatorname{Sann}(M)$.

(ii) As $\operatorname{tor}(M) = 0$ we have $\operatorname{ann}(x) = R$ for $x = 0$ and $\operatorname{ann}(x) = 0$ for $x \neq 0$. By definition $\operatorname{ann}(0) = R$ never is a prime ideal and $\operatorname{ann}(x) = 0$ is a prime ideal if and only if R is an integral domain. If $M = 0$, then R is the only annihilator ideal of M and hence $\operatorname{Sann}(M) = \emptyset$. If $M \neq 0$, then $0 \in \operatorname{Sann}(M)$ if and only if R is an integral domain. Hence the two cases.

(iii) Let us first note, that $\operatorname{ann}(M)$ is a maximal ideal of R, as we have proved in (3.24.(i)) already. Also by the definition of $\operatorname{ann}(M)$ it is clear, that

$$\operatorname{ann}(M) \;=\; \bigcap_{z \in M} \operatorname{ann}(z)$$

In particular, if $x \in M$ with $x \neq 0$ then $\operatorname{ann}(x) \neq R$ [as $1 \notin \operatorname{ann}(x)$] but we also get $\operatorname{ann}(M) \subseteq \operatorname{ann}(x) \neq R$, so by maximality of $\operatorname{ann}(M)$ we get $\operatorname{ann}(x) = \operatorname{ann}(M)$. As $x \neq 0$ has been arbitrary this proves $\operatorname{Sann}(M) \subseteq \operatorname{Anns}(M) \subseteq \{\, \operatorname{ann}(M) \,\}$. But also, as $M \neq 0$, there is some $x \in M$ with $x \neq 0$. For this x we have just seen $\operatorname{ann}(x) = \operatorname{ann}(M)$. And as $\operatorname{ann}(M)$ is maximal, it also is prime. Therefore we have $\operatorname{ann}(M) \in \operatorname{Sann}(M)$, too.

(iv) Let us consider any proper ideal $\mathfrak{a} \neq R$ of R first: In this case $\operatorname{ann}(1+\mathfrak{a}) = \{\, a \in R \mid a + \mathfrak{a} = 0 + \mathfrak{a} \,\}$ such that $\operatorname{ann}(1+\mathfrak{a}) = \{\, a \in R \mid a \in \mathfrak{a} \,\} = \mathfrak{a}$. And as $\mathfrak{a}$ is proper we have $1 + \mathfrak{a} \neq 0$ such that we conclude $\mathfrak{a} \in \operatorname{Anns}_R(R/\mathfrak{a})$.

Now we turn to prime ideals $\mathfrak{p}$ of R only. Then conversely, if $\mathfrak{b} \in \operatorname{Anns}_R(R/\mathfrak{p})$, say $\mathfrak{b} = \operatorname{ann}(b+\mathfrak{p})$ for some $b \in R$ with $b + \mathfrak{p} \neq 0 + \mathfrak{p}$. This of course is $b \notin \mathfrak{p}$. Evaluation the annihilator we find $\mathfrak{b} = \operatorname{ann}(b+\mathfrak{p}) = \{\, a \in R \mid ab + \mathfrak{p} = 0 + \mathfrak{p} \,\}$. But $ab + \mathfrak{p} = 0 + \mathfrak{p}$ is equivalent to $ab \in \mathfrak{p}$ and as $\mathfrak{p}$ is prime and $b \notin \mathfrak{p}$ this again is equivalent to $a \in \mathfrak{p}$. Altogether this means $\mathfrak{b} = \{\, a \in R \mid a \in \mathfrak{p} \,\} = \mathfrak{p}$ such that $\mathfrak{p}$ also is the only element of $\operatorname{Anns}_R(R/\mathfrak{p})$.

(v) Of course $(R/\mathfrak{a})_\mathfrak{p} = 0$ means $(b+\mathfrak{a})/v = (0+\mathfrak{a})/1$ for any $b \in R$ and any $v \notin \mathfrak{p}$. And by construction of the localization, this is $u(b+\mathfrak{a}) = 0 + \mathfrak{a}$ for some $u \notin \mathfrak{p}$. This again is $ub \in \mathfrak{a}$, altogether

$$\left(R \Big/ \mathfrak{a}\right)_\mathfrak{p} = 0 \quad\Longleftrightarrow\quad \forall\, b \in R \;\; \exists\, u \notin \mathfrak{p} \;:\; ub \in \mathfrak{a}$$

Let us first regard the case $\mathfrak{a} \subseteq \mathfrak{p}$ and take $b = 1$. Then $u \in \mathfrak{a} \subseteq \mathfrak{p}$ and $u \notin \mathfrak{p}$ is a contradiction. Therefore $(R/\mathfrak{a})_\mathfrak{p} \neq 0$ and hence $\mathfrak{p} \in \operatorname{Supp}_R(R/\mathfrak{a})$. Conversely, if $\mathfrak{a} \subseteq \mathfrak{p}$ is false, there is some $u \in \mathfrak{a}$ such that $u \notin \mathfrak{p}$. Then for any $b \in R$ we have $ub \in \mathfrak{a}$ (as $\mathfrak{a}$ is an ideal) and hence $(R/\mathfrak{a})_\mathfrak{p} = 0$. This again is $\mathfrak{p} \notin \operatorname{Supp}_R(R/\mathfrak{a})$.

Proof of (5.7):

(i) By definition $\operatorname{ann}(x) = \{\, a \in R \mid ax = 0 \,\}$. Now, as ι is injective we have $a\iota(x) = \iota(ax) = 0$ if and only if $ax = 0$. That is the following sets are identical

$$\operatorname{ann}(\iota(x)) \;=\; \{\, a \in R \mid a\iota(x) = 0 \,\} \;=\; \{\, a \in R \mid ax = 0 \,\} \;=\; \operatorname{ann}(x)$$

Therefore, if $\mathfrak{a} \in \operatorname{Anns}_R(M)$, then $\mathfrak{a} = \operatorname{ann}(x)$ for some $x \neq 0$. But as $\iota(x) \neq 0$ again, as ι is injective, this means $\mathfrak{a} = \operatorname{ann}(x) = \operatorname{ann}(\iota(x)) \in \operatorname{Anns}_R(N)$. Thus we have the inclusion $\operatorname{Anns}_R(M) \subseteq \operatorname{Anns}_R(N)$. In particular this reasoning is true if $\mathfrak{a}$ is a prime ideal of R, such that the inclusion $\operatorname{Sann}_R(M) \subseteq \operatorname{Sann}_R(N)$ is true, as well.

Consider any $\mathfrak{p} \in \mathrm{Supp}_R(M)$, that is $M_\mathfrak{p} \neq 0$. Then ι induces another monomorphism $\iota_\mathfrak{p} : M_\mathfrak{p} \hookrightarrow N_\mathfrak{p}$ according to (3.125.(ii)). In particular $N_\mathfrak{p}$ cannot be zero (this would deny $\iota_\mathfrak{p}$ to be injective) such that $\mathfrak{p} \in \mathrm{Supp}_R(N)$ again.

(ii) If $\mathfrak{a} = \mathrm{ann}(x)$ for some $x \in M$ then we regard the homomorphism of R-modules $R \to Rx : a \mapsto ax$. By construction this is surjective and $\mathfrak{a}$ is its kernel. Hence we have the isomorphism

$$R\Big/_{\mathfrak{a}} \xrightarrow{\sim} Rx \ : \ b + \mathfrak{a} \mapsto bx$$

If conversely $\Phi : R/\mathfrak{p} \xrightarrow{\sim} Rx$ is an isomorphism of R-modules, then by (i) the set of annihilators of $R/\mathfrak{p}$ and Rx are identical. But by (v) we hence find

$$\mathrm{Anns}_R(Rx) \ = \ \mathrm{Anns}_R\left(R\Big/_{\mathfrak{p}}\right) \ = \ \{\,\mathfrak{p}\,\}$$

If we have $x = 0$, then $Rx = 0$ so the isomorphy $Rx \cong_\mathrm{m} R/\mathfrak{p}$ would mean $\mathfrak{p} = R$, which contradicts R being prime. This means $x \neq 0$ and hence $\mathrm{ann}(x) \in \mathrm{Anns}_R(Rx) = \{\,\mathfrak{p}\,\}$ such that $\mathrm{ann}(x) = \mathfrak{p}$.

(iii) Abbreviate $\mathrm{Supp}(M) := \{\,\mathfrak{p} \in \mathrm{Spec}(R) \mid \exists\, x \in M : \mathrm{ann}(x) \subseteq \mathfrak{p}\,\}$. In the first step we will prove that $\mathrm{Supp}(M) \subseteq \mathbb{V}(\mathrm{ann}(M))$: As $\{\,x\,\} \subseteq M$ it is clear that $\mathrm{ann}(M) \subseteq \mathrm{ann}(x)$ and by assumption any $\mathfrak{p} \in \mathrm{Supp}(M)$ satisfies $\mathrm{ann}(M) \subseteq \mathrm{ann}(x) \subseteq \mathfrak{p}$ for some $x \in M$. Therefore (by choosing this $x \in M$) $\mathrm{ann}(M) \subseteq \mathfrak{p}$ which is $\mathfrak{p} \in \mathbb{V}(\mathrm{ann}(M))$.

In the next step we will prove $\mathbb{V}(\mathrm{ann}(M)) \subseteq \{\,\mathfrak{p} \in \mathrm{Spec}(R) \mid M_\mathfrak{p} \neq 0\,\}$. So what does $M_\mathfrak{p} = 0$ mean? By definition this is $x/v = 0/1$ for any $x \in M$ and any $v \notin \mathfrak{p}$. And this again is: For any $x \in M$ there is some $u \notin \mathfrak{p}$ such that $ux = 0$. So if we start with some $\mathfrak{p} \in \mathbb{V}(\mathrm{ann}(M))$, then we have $\mathrm{ann}(M) \subseteq \mathfrak{p}$. In particular $u \notin \mathfrak{p}$ implies $u \notin \mathrm{ann}(M)$. And by definition of $\mathrm{ann}(M)$ this is $ux \neq 0$ for some $x \in M$ - just what we needed, for $M_\mathfrak{p} \neq 0$.

In the last step we will prove $\{\,\mathfrak{p} \in \mathrm{Spec}(R) \mid M_\mathfrak{p} \neq 0\,\} \subseteq \mathrm{Supp}(M)$. That is we start with some prime ideal $\mathfrak{p}$ such that $M_\mathfrak{p} \neq 0$ and need to prove that there is some $x \in M$ such that $\mathrm{ann}(x) \subseteq \mathfrak{p}$. That is we have to show that $u \in \mathrm{ann}(x)$ - which is $ux = 0$ - implies $u \in \mathfrak{p}$. As we have argued above $M_\mathfrak{p} = 0$ means $\forall\, x \in M\ \exists\, u \notin \mathfrak{p}$ such that $ux = 0$. The negation thereof is $\exists\, x \in M\ \forall\, u \notin \mathfrak{p}$ we get $ux \neq 0$. Yet $u \notin \mathfrak{p} \implies ux \neq 0$ is equivalent to $ux = 0 \implies u \in \mathfrak{p}$. Thus there is some $x \in M$ such that $u \in \mathrm{ann}(x)$ implies $u \in \mathfrak{p}$ which is just what we needed: $\mathrm{ann}(x) \subseteq \mathfrak{p}$.

(iv) By definition $\mathrm{ann}(x) = \{\,a \in R \mid ax = 0\,\}$ and if we rewrite the quantifier $\exists\, x \in M : x \neq 0$ as a union over all $x \in M$ with $x \neq 0$ the identity of these sets is readily apparent

$$\mathrm{zd}(M) \ = \ \bigcup_{x \neq 0} \{\,a \in R \mid ax = 0\,\} \ = \ \bigcup_{x \neq 0} \mathrm{ann}(x) \ = \ \bigcup \mathrm{Anns}(M)$$

(v) Let $\mathfrak{a} = \mathrm{ann}(x)$ for some $x \neq 0$ and consider $a, b \in R$ such that $ab \in \mathfrak{a}$ and $b \notin \mathfrak{a}$. Then we need to prove $a \in \mathfrak{a}$. By assumption we have $abx = 0$ and $bx \neq 0$, that is $a \in \mathrm{ann}(bx) \in \mathrm{Anns}(M)$. But clearly $\mathfrak{a} = \mathrm{ann}(x) \subseteq \mathrm{ann}(bx)$, as R is commutative. By maximality of $\mathfrak{a}$ this implies $\mathfrak{a} = \mathrm{ann}(bx)$ and hence $a \in \mathfrak{a}$, which had to be proved.

□

Proof of (5.8):

(i) If $\mathfrak{p} = \mathrm{ann}(x) \in \mathrm{Sann}(P)$, then as $0 \neq x \in P \subseteq M$ we already find $\mathfrak{p} = \mathrm{ann}(x) \in \mathrm{Sann}(M)$. Thereby we already have the inclusion

$$\mathrm{Sann}(P) \quad \subseteq \quad \mathrm{Sann}(M)$$

Now consider any $x \in M$ and distinguish two cases: If $Rx \cap P = 0$ (as $ax \in Rx$ is generally true) then $ax \in P$ is equivalent to $ax \in Rx \cap P = 0$ and hence to $ax = 0$. Therefore

$$\begin{aligned} \mathrm{ann}(x+P) &= \{\, a \in R \mid a(x+P) = 0 \in M/P \,\} \\ &= \{\, a \in R \mid ax \in P \,\} \\ &= \{\, a \in R \mid ax = 0 \,\} \;=\; \mathrm{ann}(x) \end{aligned}$$

In particular $\mathrm{ann}(x) = \mathrm{ann}(x+P) \in \mathrm{Sann}(M/P)$. In the complementary case $Rx \cap P \neq 0$ there is some $y = bx \in P$ such that $y \neq 0$. In particular $b \notin \mathrm{ann}(x) = \mathfrak{p}$. Then (3.24.(ii)) tells us that $\mathrm{Anns}(Ry) = \{\, \mathfrak{p} \,\}$ and in particular $\mathrm{ann}(y) = \mathfrak{p} = \mathrm{ann}(x)$. That is $\mathrm{ann}(x) = \mathrm{ann}(y) \in \mathrm{Sann}(P)$. Together we have found

$$\mathrm{Sann}(M) \;\subseteq\; \mathrm{Sann}(P) \cup \mathrm{Sann}\left(M \Big/ P\right)$$

(i) If $0 \to L \to M \to N \to 0$ is an exact chain of R-modules, let us denote the respective homomorphisms by $\varphi : L \hookrightarrow M$ and $\psi : M \twoheadrightarrow N$. Then $L \xrightarrow{\sim} \mathrm{im}(\varphi) = \mathrm{kn}(\psi)$ due to exactness, such that

$$\mathrm{Sann}(L) \;=\; \mathrm{Sann}(\mathrm{kn}(\psi)) \quad \subseteq \quad \mathrm{Sann}(M)$$

as $P := \mathrm{kn}(\psi) \;\leq_{\mathfrak{m}}\; M$ is a sub-module of M and we have (i) above. Also the first isomorphism theorem implies $M/\mathrm{kn}(\psi) \xrightarrow{\sim} \mathrm{im}(\psi) = N$ such that (i) above also implies

$$\mathrm{Sann}(M) \;\subseteq\; \mathrm{Sann}(\mathrm{kn}(\psi)) \cup \mathrm{Sann}\left(M \Big/ \mathrm{kn}(\psi)\right) \;=\; \mathrm{Sann}(L) \cup \mathrm{Sann}(N)$$

(ii) As any $P_i \;\leq_{\mathfrak{m}}\; M$ is a sub-module, we have $\mathrm{Sann}(P_i) \subseteq \mathrm{Sann}(M)$ by (vi). Therefore $\bigcup_i \mathrm{Sann}(P_i)$ is contained in $\mathrm{Sann}(M)$. Conversely consider any $\mathfrak{p} = \mathrm{ann}(x) \in \mathrm{Sann}(M)$. As $x \in M = \bigcup_i P_i$ there is some $i \in I$ such that $x \in P_i$ and thereby $\mathfrak{p} = \mathrm{ann}(x) \in \mathrm{Sann}(P_i)$. That is $\mathrm{Sann}(M)$ also is contained in $\bigcup_i \mathrm{Sann}(P_i)$.

(iv) If $\#I = 1$ then there is nothing to prove. If $\#I = 2$, say $I = \{\, 1, 2 \,\}$ we abbreviate $M := M_1 \oplus M_2$. As $M_1 \subseteq M$ (canonically under $x_1 \mapsto (x_1, 0)$ we have $\mathrm{Sann}(M_1) \subseteq \mathrm{Sann}(M)$ according to (iv). Likewise $\mathrm{Sann}(M_2) \subseteq \mathrm{Sann}(M)$. And clearly $M/M_1 \xrightarrow{\sim} M_2 : (x_1, x_2) + M_1 \mapsto x_2$ is an isomorphism and hence we may apply (iv) to find

$$\begin{aligned} \mathrm{Sann}(M) &\subseteq \mathrm{Sann}(M_1) \cup \mathrm{Sann}\left(M \Big/ M_1\right) \\ &= \mathrm{Sann}(M_1) \cup \mathrm{Sann}(M_2) \end{aligned}$$

But as we also have $\mathrm{Sann}(M_1) \cup \mathrm{Sann}(M_2) \subseteq \mathrm{Sann}(M)$ we have the equality of these sets. Thus we have proved the claim for $\#I = 2$. Now suppose I is a finite set, then we may use induction on $n := \#I$. The cases $n = 1$ and $n = 2$ have already been dealt with. For the induction step we consider $I = 1 \ldots (n+1)$ and let $M := Q \oplus M_{n+1}$ where $Q := M_1 \oplus \cdots \oplus M_n$. Then we may use

the case $n = 2$ on M and the induction hypothesis on Q to find

$$\begin{aligned}\mathrm{Sann}(M) &= \mathrm{Sann}(Q) \cup \mathrm{Sann}(M_{n+1}) \\ &= \bigcup_{i=1}^{n} \mathrm{Sann}(M_i) \cup \mathrm{Sann}(M_{n+1}) = \bigcup_{i=1}^{n+1} \mathrm{Sann}(M_i)\end{aligned}$$

For an infinite index set I we finally let $\Omega := \{ A \subseteq I \mid A \neq \emptyset, \#A < \infty \}$. Then for some non-empty finite subset $A \in \Omega$ of I we let

$$\begin{aligned}M &:= \bigoplus_{i \in A} M_i \\ M_A &:= \bigoplus_{i \in A} M_i \quad \leq_{\mathfrak{m}} \quad M\end{aligned}$$

By construction any $x \in M$ is contained in some $x \in M_A$ for some $A \in \Omega$. That is $M = \bigcup_A M_A$ where the union runs over $A \in \Omega$. Now by (ii) the annihilator spectrum if the union of the annihilator spectra of M_A and as A is finite these are given to be

$$\mathrm{Sann}(M) = \bigcup_{A \in \Omega} \mathrm{Sann}(M_A) = \bigcup_{A \in \Omega} \bigcup_{i \in A} \mathrm{Sann}(M_i) = \bigcup_{i \in I} \mathrm{Sann}(M_i)$$

(iii) By assumption the following map is injective: If $(x + P_i) = 0 = (0 + P_i)$ then we have $x \in P_i$ for any $i \in I$. But as $x \in \bigcup_i P_i = 0$ is $x = 0$ we find the injectivity, of

$$M \hookrightarrow \bigoplus_{i \in I} M \big/ P_i \; : \; x \mapsto (x + P_i)$$

That is we can consider M as a sub-module of the direct sum of the M/P_i and by (i) and (iv) this implies our claim

$$\mathrm{Sann}(M) \subseteq \mathrm{Sann}\left(\bigoplus_{i \in I} M \big/ P_i \right) = \bigcup_{i \in I} \mathrm{Sann}\left(M \big/ P_i \right)$$

(v) As $\mathfrak{p} \in \mathrm{Spec}(R)$ already is a prime ideal, we have $\mathfrak{p} \in \mathrm{Sann}(M)$ if and only if $\mathfrak{p} \in \mathrm{Anns}(M)$. But as $\mathfrak{p} \neq R$ is proper this is equivalent to the existence of ι according to (3.22.(ii)).

(vi) If $M = 0$ then there is no $x \in M$ with $x \neq 0$. Therefore $\mathrm{Sann}(M) = \emptyset$ by construction. Conversely if $M \neq 0$ then there is some $x \in M$ with $x \neq 0$. That is $1 \notin \mathrm{ann}(x)$ and thereby $\mathrm{ann}(x) \neq R$. In particular $\mathcal{A} := \mathrm{Anns}(M) \neq \emptyset$. As R is noetherian and $\mathcal{A}$ is non-empty we get $\mathcal{A}^* \neq \emptyset$ as well. And as the maximal elements of $\mathcal{A}$ are prime ideals by (3.24.(iii)) we have $\emptyset \neq \mathcal{A}^* \subseteq \mathrm{Spec}(R) \cap \mathrm{Anns}(M) = \mathrm{Sann}(M)$.

(vii) First of all, we regard the case $M = 0$: Here $\mathrm{Sann}(M) = \emptyset$ and hence the grand union of $\mathrm{Sann}(M)$ is empty, too. But also $\mathrm{zd}(M) = \emptyset$, as there is no $x \neq 0$ to begin with. That is in case $M = 0$ we have the equality and may assume $M \neq 0$ from now on:

If $\mathfrak{p} \in \mathrm{Sass}(M)$ is an associated prime of M, then $\mathfrak{p} = \mathrm{ann}(x)$ for some $x \neq 0$. That is any $a \in \mathfrak{p}$ satisfies $ax = 0$ and as $x \neq 0$ this means $a \in \mathrm{zd}(M)$. Hence $\mathfrak{p} \subseteq \mathrm{zd}(M)$ which is "$\subseteq$" above.

For the converse inclusion we start with some $a \in \mathrm{zd}(M)$, that is there is some $x \neq 0$ such that $ax = 0$. In particular $Rx \neq 0$ such that by (vi) there is some $\mathfrak{p} \in \mathrm{Sann}(Rx) \subseteq \mathrm{Sann}(M)$. Say $\mathfrak{p}$ is $\mathfrak{p} = \mathrm{ann}(bx)$ for some $bx \neq 0$. Then $a(bx) = b(ax) = b \cdot 0 = 0$ such that $a \in \mathfrak{p} \in \mathrm{Sann}(M)$. That is a is contained in the grand union of $\mathrm{Sann}(M)$.

(viii) Let $\mathcal{Z} := \{\, Z \leq_{\mathfrak{m}} M \mid \mathrm{Sann}(Z) \subseteq \mathcal{S} \,\}$ be the set of sub-modules of M whose annihilator spectrum is contained in $\mathcal{S}$. From (vi) we know $\mathrm{Sann}(0) = \emptyset \subseteq \mathcal{S}$ such that $0 \in \mathcal{Z}$ which tells us that $\mathcal{Z}$ is non-empty. And if $(Z_i) \subseteq \mathcal{Z}$ is a chain then $Z := \bigcup_i Z_i$ is a sub-module by (3.13). Also we have

$$\mathrm{Sann}(Z) \;=\; \bigcup_{i \in I} \mathrm{Sann}(Z_i) \;\subseteq\; \mathcal{S}$$

according to (ii). This means $Z \in \mathcal{Z}$ again and thereby any chain in $\mathcal{Z}$ has an upper bound such that we may apply the lemma of Zorn (0.29) to find a maximal element $P \in \mathcal{Z}^*$. As $P \in \mathcal{Z}$ we have $\mathrm{Sann}(P) \subseteq \mathcal{S}$. Let us now argue, that

$$\mathrm{Sann}\left(M \Big/ P\right) \cap \mathcal{S} \;=\; \emptyset$$

Consider any $\mathfrak{p} \in \mathrm{Sann}(M/P)$ then we have a monomorphism of the form $\iota : R/\mathfrak{p} \hookrightarrow M/P$ by (v). Let $Q/P := \mathrm{im}(\iota)$ be the image of this, that is $Q \leq_{\mathfrak{m}} M$ with $P \subseteq Q$. Then $\iota : R/\mathfrak{p} \xrightarrow{\sim} Q/P$ is an isomorphism. In particular $\mathrm{Sann}(Q/P) = \mathrm{Sann}(R/\mathfrak{p}) = \{\, \mathfrak{p} \,\}$ and by (i) we hence get

$$\mathrm{Sann}(Q) \;\subseteq\; \mathrm{Sann}(P) \cup \mathrm{Sann}\left(Q \Big/ P\right) \;=\; \mathrm{Sann}(P) \cup \{\, \mathfrak{p} \,\}$$

If we had $\mathfrak{p} \in \mathcal{S}$ as well, then this would mean $\mathrm{Sann}(Q) \subseteq \mathcal{S}$. But as P is maximal with this property and $P \subseteq Q$ this would yield $P = Q$ which contradicts $Q/P \cong_{\mathfrak{m}} R/\mathfrak{p} \neq 0$. Thus $\mathcal{S}$ and $\mathrm{Sann}(M/P)$ are disjoint. But from this we will find

$$\mathrm{Sann}(P) \;=\; \mathcal{S}$$

We already have $\mathrm{Sann}(P) \subseteq \mathcal{S}$, so let us suppose there was some $\mathfrak{p} \in \mathcal{S} \setminus \mathrm{Sann}(P)$. As $\mathfrak{p} \in \mathcal{S} \subseteq \mathrm{Sann}(M) \subseteq \mathrm{Sann}(P) \cup \mathrm{Sann}(M/P)$ but $\mathfrak{p} \notin \mathrm{Sann}(P)$ we necessarily have $\mathfrak{p} \in \mathrm{Sann}(M/P)$. But this cannot be, as $\mathcal{S}$ and $\mathrm{Sann}(M/P)$ are disjoint, which only leaves $\mathrm{Sann}(P) = \mathcal{S}$. And thereby

$$\mathrm{Sann}(M) \setminus \mathcal{S} \;=\; \mathrm{Sann}(M) \setminus \mathrm{Sann}(P) \;\subseteq\; \mathrm{Sann}\left(M \Big/ P\right)$$

□

Proof of (5.12):

(i) Recall the canonical map $\kappa : R \to U^{-1}R : a \mapsto a/1$. By definition $U^{-1}\mathrm{ann}(x)$ is the ideal of $U^{-1}R$ generated by $\kappa(\mathrm{ann}(x))$

$$\begin{aligned} U^{-1}\mathrm{ann}(x) &= \langle \left\{ \frac{a}{1} \mid a \in \mathrm{ann}(x) \right\} \rangle_{\mathfrak{i}} \\ &= \langle \left\{ \frac{a}{1} \mid a \in R,\, ax = 0 \right\} \rangle_{\mathfrak{i}} \end{aligned}$$

Likewise $\mathrm{ann}(x/1) \trianglelefteq_{\mathfrak{i}} U^{-1}R$ is the set of all $a/u \in U^{-1}R$ such that $ax/u = a/u\,x/1 = 0/1$. The

latter is equivalent to: $wax = wu0 = 0$ for some $w \in U$. That is

$$\operatorname{ann}\left(\frac{x}{1}\right) \;=\; \left\{ \frac{a}{u} \in U^{-1}R \mid \exists\, w \in U \,:\, wax = 0 \right\}$$

We will now prove that (under the assumption $\mathfrak{p} = \operatorname{ann}(x)$ is a prime ideal, with $\mathfrak{p} \cap U = \emptyset$) these sets are equal: For $U^{-1}\operatorname{ann}(x) \subseteq \operatorname{ann}(x/1)$ we consider some $a \in R$ with $ax = 0$. Then clearly $a/1 \in \operatorname{ann}(x/1)$, as we have $wax = 0$ for $w = 1 \in U$. And as $\operatorname{ann}(x/1)$ is an ideal, it therefore contains $U^{-1}\operatorname{ann}(x)$.

Conversely we take a look some a/u such that $wax = 0$ for some $w \in U$. That means $wa \in \operatorname{ann}(x) = \mathfrak{p}$. As $w \in U$ we have $w \notin \mathfrak{p}$ and as $\mathfrak{p}$ is a prime ideal, this implies $a \in \mathfrak{p} = \operatorname{ann}(x)$. That is $ax = 0$ and hence $a/1 \in U^{-1}\operatorname{ann}(x)$. But as this is an ideal, we also have $a/u = (1/u) \cdot (a/1) \in U^{-1}\operatorname{ann}(x)$.

(ii) We have already seen in (2.129) that $\mathfrak{p} \mapsto U^{-1}\mathfrak{p}$ is a bijective map from $\mathcal{S} := \{\, \mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \cap U = \emptyset \,\}$ to $\operatorname{Spec}(U^{-1}R)$. So if $\mathfrak{p} = \operatorname{ann}(x) \in \operatorname{Sann}(M)$ with $\mathfrak{p} \cap U = \emptyset$, then by (i) we see that $U^{-1}\mathfrak{p} = \operatorname{ann}(x/1) \in \operatorname{Sann}(U^{-1}M)$. Hence the map is well-defined and its injectivity is inherited from the bijectivity on the spectrum.

(iii) By assumption $\mathfrak{p} = \langle a_1, \ldots, a_n \rangle_{\mathfrak{i}} \trianglelefteq_{\mathfrak{i}} R$ is finitely generated and $U^{-1}\mathfrak{p} = \operatorname{ann}(x/u)$ is the annihilator of some element $x/u \in U^{-1}M$. As in (i) this ideal can be explicitly written, as

$$\operatorname{ann}\left(\frac{x}{u}\right) \;=\; \left\{ \frac{b}{v} \in U^{-1}R \mid \exists\, w \in U \,:\, wbx = 0 \right\}$$

For any $k \in 1 \ldots n$ we have $a_k \in \mathfrak{p}$ and therefore $a_k/1 \in U^{-1}\mathfrak{p} = \operatorname{ann}(x/u)$ which means $(a/1)\,(x/u) = 0/1$ and this is $w_k a_k x = 0$ for some $w_k \in U$. Now let $w := w_1 \ldots w_n \in U$ then clearly $a_k(wx) = wa_k x = 0$ for any $k \in 1 \ldots n$. This means $a_k \in \operatorname{ann}(wx)$ and as the a_k generate $\mathfrak{p}$ we even get the inclusion

$$\mathfrak{p} \;\subseteq\; \operatorname{ann}(wx)$$

Conversely, if $b \in \operatorname{ann}(wx)$ then $wbx = bwx = 0$ which means $b/1 \in \operatorname{ann}(x/u) = U^{-1}\mathfrak{p}$. But this implies $b \in U^{-1}\mathfrak{p} \cap R = \mathfrak{p}$ such that we also have $\operatorname{ann}(wx) \subseteq \mathfrak{p}$. But together this is $\mathfrak{p} = \operatorname{ann}(wx) \in \operatorname{Sann}(M)$ as claimed.

(ii) Now consider any $\mathfrak{q} \in \operatorname{Sann}(U^{-1}M) \subseteq \operatorname{Spec}(U^{-1}R)$. As the map is bijective on the spectrum, there is some $\mathfrak{p} \in \operatorname{Spec}(R)$ such that $\mathfrak{p} \cap U = \emptyset$ and $\mathfrak{q} = U^{-1}\mathfrak{p}$. If R is noetherian, then $\mathfrak{p}$ is finitely generated and hence we may apply (iii) to get $\mathfrak{p} \in \operatorname{Sann}(M)$. That is $\mathfrak{p} \mapsto U^{-1}\mathfrak{p} = \mathfrak{q}$ and hence this map also is surjective.

(iv) By (5.8.(vii)) there is a sub-module $Q \leq_{\mathfrak{m}} M$ that satisfies $\operatorname{Sann}(Q) = \operatorname{Sann}(M) \setminus \mathcal{S}$ and $\operatorname{Sann}(Q) \cap \operatorname{Sann}(M/Q) = \emptyset$. By definition of $\mathcal{S}$ this means, that for any $\mathfrak{p} \in \operatorname{Sann}(M)$ we have

$$\mathfrak{p} \in \operatorname{Sann}(Q) \iff \mathfrak{p} \notin \mathcal{S} \iff \mathfrak{p} \cap U \neq \emptyset$$

And as by (5.8.(i)) any $\mathfrak{p} \in \operatorname{Sann}(M)$ is contained in either $\operatorname{Sann}(Q)$ or in $\operatorname{Sann}(M/Q)$ this means $\operatorname{Sann}(M/Q) = \mathcal{S}$. Now let us also denote $\kappa : M \to U^{-1}M : x \mapsto x/1$ and $P := \operatorname{kn}(\kappa)$. Then we

regard the following commutative diagram

$$\begin{array}{ccc} M & \xrightarrow{\varrho} & M/Q \\ \downarrow & & \downarrow \\ U^{-1}M & \underset{U^{-1}\varrho}{\longrightarrow} & U^{-1}(M/Q) \end{array}$$

where κ and $\overline{\kappa} : M/Q \to U^{-1}(M/Q) : x+Q \mapsto (x+Q)/1$ are the canonical homomorphisms downwards and $\varrho : M \to M/Q : x \mapsto x+Q$ is the canonical projection. By definition $U^{-1}\varrho : U^{-1}M \to U^{-1}(M/Q)$ is defined by $U^{-1}\varrho(x/u) := (x+Q)/u$. This diagram commutes, as

$$\overline{\kappa}\varrho(x) \;=\; \frac{x+Q}{1} \;=\; \big(U^{-1}\varrho\big)\kappa(x)$$

We first claim, that $U^{-1}\varrho$ is injective: That is we need to show that $\mathrm{kn}(U^{-1}\varrho) = 0$. Hereby (3.125.(ii)) tells us $\mathrm{kn}(U^{-1}\varrho) = U^{-1}\mathrm{kn}(\varrho) = U^{-1}Q$. And as R is noetherian we know by (ii) that $\mathrm{Sann}(U^{-1}Q)$ is bijective to $\{\,\mathfrak{p} \in \mathrm{Sann}(Q) \mid \mathfrak{p} \cap U = \emptyset\,\} = \emptyset$. But by construction of $\mathcal{S}$ and Q the latter set is void and hence $\mathrm{Sann}(U^{-1}Q) = \emptyset$ is empty, as well. But by (5.8.(vi)) this means $\mathrm{kn}(U^{-1}\varrho) = U^{-1}Q = 0$, such that $U^{-1}\varrho$ is injective.

Next we claim, that $\overline{\kappa}$ is injective, as well: To do this let $K/Q := \mathrm{kn}(\overline{\kappa}) \;\leq_{\mathfrak{m}}\; M/Q$, then $\mathrm{Sann}(K/Q) \subseteq \mathrm{Sann}(M/Q) = \mathcal{S}$. Now consider any $\mathfrak{p} \in \mathrm{Sann}(K/Q)$, that is $\mathfrak{p} = \mathrm{ann}(x+Q)$ for some $x \in K \;\leq_{\mathfrak{m}}\; M$. As $x+Q \in \mathrm{kn}(\overline{\kappa})$ we have $(x+Q)/1 = 0/1 \in U^{-1}(M/Q)$ and this means $w(x+Q) = 0+Q$ for some $w \in U$. That is $w \in U$ annihilates $x+Q$ such that $w \in \mathrm{ann}(x+Q) \cap U = \mathfrak{p} \cap U$. But as $\mathfrak{p} \in \mathcal{S}$ we have $\mathfrak{p} \cap U = \emptyset$. This contradiction can only be solved, if there is no $\mathfrak{p} \in \mathrm{Sann}(K/Q)$ which means $\mathrm{Sann}(K/Q) = 0$. Using (5.8.(vi)) again this is $\mathrm{kn}(\overline{\kappa}) = K/Q = 0$, such that $\overline{\kappa}$ is injective.

Using both injectivities we find $Q = P$ (see below). And as Q has been *any* sub-module of M satisfying $\mathrm{Sann}(Q) = \mathrm{Sann}(M) \setminus \mathcal{S}$ and $\mathrm{Sann}(Q) \cap \mathrm{Sann}(M/Q) = \emptyset$ this proves the uniqueness of Q. Also P inherits these properties from Q.

$$Q \;=\; \mathrm{kn}(\varrho) \;=\; \mathrm{kn}(\overline{\kappa}\varrho) \;=\; \mathrm{kn}\Big(\big(U^{-1}\varrho\big)\kappa\Big) \;=\; \mathrm{kn}(\kappa) \;=\; P$$

□

Proof of (5.13):
Let $S := R_{\mathfrak{p}}$ abbreviate the localisation of R in $\mathfrak{p}$, then S is noetherian, too, according to (2.131). Also $M_{\mathfrak{p}} \neq 0$, as $\mathfrak{p} \in \mathrm{Supp}(M)$ such that $\mathrm{Sann}_S(M_{\mathfrak{p}}) \neq \emptyset$ is non-empty, by (5.8.(vi)). But (5.12.(ii)) tells us, that there is a one-to-one correspondence between the sets

$$\mathrm{Sann}_S\,(M_{\mathfrak{p}}) \;\longleftrightarrow\; \{\,\mathfrak{a} \in \mathrm{Sann}_R(M) \mid \mathfrak{a} \cap (R \setminus \mathfrak{p}) = \emptyset\,\}$$

As the left-hand set is non-empty, so is the right-hand set, that is there is some $\mathfrak{a} \in \mathrm{Sann}(M)$ such that $\mathfrak{a} \cap (R \setminus \mathfrak{p}) = \emptyset$. But the latter property translates into $\mathfrak{a} \subseteq \mathfrak{p}$.

Consider any $\mathfrak{a} = \mathrm{ann}(x) \in \mathrm{Sann}(M)$, that is $x \neq 0$ and $\mathfrak{a}$ is prime. In particular $\mathrm{ann}(x) \subseteq \mathfrak{a} \in \mathrm{Spec}(R)$,

such that $\mathfrak{a} \in \mathrm{Supp}(M)$, by construction of the support. From this we see the inclusion

$$\mathrm{Sann}(M) \quad \subseteq \quad \mathrm{Supp}(M)$$

It remains to prove that the minimal elements of these sets coincide. If $\mathfrak{p} \in \mathrm{Supp}(M)$ is minimal, then we choose some $\mathfrak{a} \in \mathrm{Sann}(M)$ such that $\mathfrak{a} \subseteq \mathfrak{p}$. As $\mathfrak{a} \in \mathrm{Supp}(M)$, too and $\mathfrak{p}$ is minimal in this set we find $\mathfrak{a} = \mathfrak{p}$, in particular $\mathfrak{p} \in \mathrm{Sann}(M)$ is an associated prime of M. And clearly it is minimal in $\mathrm{Sann}(M)$, as any $\mathrm{Sann}(M)$ is contained in $\mathrm{Supp}(M)$.
Conversely if $\mathfrak{a} \in \mathrm{Sann}(M)$ is minimal, then we already know $\mathfrak{a} \in \mathrm{Supp}(M)$, but have to show, that it also is minimal in this set. That is we consider some $\mathfrak{p} \in \mathrm{Supp}(M)$ such that $\mathfrak{p} \subseteq \mathfrak{a}$ and have to show $\mathfrak{a} = \mathfrak{p}$. Again choose some $\mathfrak{b} \in \mathrm{Sann}(M)$ such that $\mathfrak{b} \subseteq \mathfrak{p} \subseteq \mathfrak{a}$. As $\mathfrak{a}$ is minimal in $\mathrm{Sann}(M)$ and $\mathfrak{b} \in \mathrm{Sann}(M)$ we conclude $\mathfrak{a} = \mathfrak{b}$ and thereby $\mathfrak{a} = \mathfrak{p}$.
We have just shown, that the minimal elements of $\mathrm{Sann}(M)$ and $\mathrm{Supp}(M)$ coincide. For the grand intersection only minimal elements are relevant, though [if $\mathfrak{p} \in \mathrm{Sann}(M)$ is *not* minimal, then there is some $\mathfrak{p} \subseteq \mathfrak{q}$. And hence $\mathfrak{q}$ does not contribute to the intersection: $\mathfrak{p} \cap \mathfrak{q} = \mathfrak{p}$. The same is true for $\mathrm{Sann}(M)$ of course]. Thus we find

$$\bigcap \mathrm{Sann}(M) \;=\; \bigcap \big(\mathrm{Sann}(M)\big)_* \;=\; \bigcap \big(\mathrm{Supp}(M)\big)_* \;=\; \bigcap \mathrm{Supp}(M)$$

□

Proof of (5.11):

(i) By definition $M = M(p) = \{\, x \in M \mid \exists\, n \in \mathbb{N} : p^n x = 0 \,\}$. Yet Yet the condition in this set can be reformulated to $\exists\, n \in \mathbb{N} : p^n \in \mathrm{ann}(x)$ which in turn is $p \in \sqrt{\mathrm{ann}(x)}$. That is

$$M(p) \quad = \quad \left\{ x \in M \mid p \in \sqrt{\mathrm{ann}(x)} \right\}$$

Consider any $\mathfrak{p} \in \mathrm{Sann}(M)$, that is $\mathfrak{p} = \mathrm{ann}(x)$ for some $x \neq 0$, then $M = M(p)$ tells us $p \in \sqrt{\mathrm{ann}(x)}$ which is $pR \subseteq \sqrt{\mathrm{ann}(x)} = \mathrm{ann}(x)$ - the latter, as $\mathrm{ann}(x)$ is prime. Thus we have $p \in \mathrm{ann}(x)$. And as $x \neq 0$ we know $\mathrm{ann}(x) \neq R$ such that we have found

$$pR \quad \subseteq \quad \mathrm{ann}(x) \quad \neq \quad R$$

As R is a PID the non-zero prime ideal pR is maximal, according to (2.79.(i)) such that we find $\mathfrak{p} = \mathrm{ann}(x) = pR$ by the inclusion above. That is we have shown $\mathrm{Sann}(M) \subseteq \{\, pR \,\}$. On the other hand $M \neq 0$ is finitely generadet (by assumption) such that from (5.8.(vi)) we have $\mathrm{Sann}(M) \neq \emptyset$. But this leaves $\mathrm{Sann}(M) = \{\, pR \,\}$ only.

(ii) By (5.13) we know $\mathrm{Sann}(R/aR) \subseteq \mathrm{Supp}(R/aR)$ and by (5.6.(iv)) this is $\mathbb{V}(aR)$ such that we find

$$\begin{aligned} \mathrm{Sann}\left(R\big/_{aR}\right) \quad &\subseteq \quad \mathrm{Supp}\left(R\big/_{aR}\right) \\ &= \quad \mathbb{V}(aR) \;=\; \{\, pR \mid p \in R \text{ prime}, aR \subseteq pR \,\} \\ &= \quad \{\, pR \mid p \in R \text{ prime}, p \mid a \,\} \end{aligned}$$

For the converse inclusion we start with any prime $p \in R$ such that $p \mid a$, that is $pu = a$ for some

$u \in R$. As $a \neq 0$ so is $u \neq 0$. Now let $x := u + aR$. Suppose $x = 0$, then $u \in aR$, say $u = ab$ for some $b \in R$, then $u = ab = pub$ such that $1 = pb$ (as $u \neq 0$) which would be $p \in R^*$, in contradiction to p being prime. Thus $x \neq 0$ but $px = p(u + aR) = pu + aR = a + aR = 0 + aR$. That is $p \in \mathrm{ann}(x)$, i.e. $pR \subseteq \mathrm{ann}(x) \neq R$ (as in (i) above) such that we find $\mathrm{ann}(x) = pR$ again. In particular $\mathrm{ann}(x)$ is prime and hence $pR = \mathrm{ann}(x) \in \mathrm{Sann}(R/aR)$.

□

Proof of (5.14):

- First consider the case $M = 0$, then statement (2) is void and statement (1) is trivial for $n = 0$ and $M_0 = 0 = M$. So let us now deal with $M \neq 0$, as R is noetherian and M is finitely generated, M is noetherian, too, according to (3.111.(vi)). Hence we consider the set of all sub-modules of M that do satify properties (1) and (2) of the claim.

 First of all, this set is nonempty: As $M \neq 0$ there is some $\mathfrak{p} \in \mathrm{Sann}(M)$, due to (5.8.(vi)). Say $\mathfrak{p} = \mathrm{ann}(x)$ then $R/\mathfrak{p} \cong_{\mathsf{m}} Rx : a + \mathfrak{p} \mapsto ax$ is an isomorphism of R-modules and thereby Rx satisfies properties (1) and (2), as we may take $0 = M_0 \subset M_1 = Rx$ such that $M_1/M_0 \cong_{\mathsf{m}} Rx \cong_{\mathsf{m}} R/\mathfrak{p}$. Hence $Rx \leq_{\mathsf{m}} M$ is one of those sub-modules.

 As the set of sub-modules satisfying (1) and (2) is non-empty and M is noetherian, there is a maximal sub-module N satisfying (1) and (2). In particular there are some N_i and $\mathfrak{p}_i$ as in (1) and (2). We need to prove $N = M$, so suppose this was *not* the case: $N \subset M$. Then $M/N \neq 0$ and therefore $\mathrm{Sann}(M/N) \neq \emptyset$ again. Let $\mathfrak{p} = \mathrm{ann}(x + N)$ be an associated prime ideal of M/N, then we find the chain of sub-modules

$$0 = N_0 \subset N_1 \subset \ldots \subset N_n = N \subset N + Rx$$

 Also we have $R/\mathfrak{p} \cong_{\mathsf{m}} R(x + N) : a + \mathfrak{p} \mapsto ax + N$ as before. And as $(Rx + N)/N = R(x + N)$ we have found an extension of the chain $0 = N_0 \subset \ldots \subset N_n = N$ in contradiction to the maximality of N. But this only leaves $M/N = 0$, in other words $N = M$.

- We prove $\mathrm{Sann}(M) \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ by induction on n: In case $n = 0$, which is $M = 0$, we have $\mathrm{Sann}(M) = \emptyset$. Now consider $n = 1$ which is $0 = M_0 \subset M_1 = M$. Then we get

$$\mathrm{Sann}(M) = \mathrm{Sann}(M_1) = \mathrm{Sann}\left(M_1 \big/ M_0\right) = \mathrm{Sann}\left(R \big/ \mathfrak{p}_1\right) = \{\mathfrak{p}_1\}$$

 Now suppose we have already proved the claim for all modules with filtrations of length less than n. That is we have $\mathrm{Sann}(M_{n-1}) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_{n-1}\}$ by induction hypothesis and then we find

$$\begin{aligned} \mathrm{Sann}(M) &= \mathrm{Sann}(M_n) \subseteq \mathrm{Sann}(M_{n-1}) \cup \mathrm{Sann}\left(M_n \big/ M_{n-1}\right) \\ &= \mathrm{Sann}(M_{n-1}) \cup \mathrm{Sann}\left(R \big/ \mathfrak{p}_n\right) \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_{n-1}\} \cup \{\mathfrak{p}_n\} \end{aligned}$$

- For the inclusion $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \subseteq \mathrm{Supp}(M)$ we start with any $i \in 1 \ldots n$: By property (2) there is some isomorphism $\Phi_i : M_i/M_{i-1} \xrightarrow{\sim} R/\mathfrak{p}_i$ such that we may pick up $x_i \in M_i \subseteq M$ such that $\Phi_i(x_i + M_{i-1}) = 1 + \mathfrak{p}_i$. If now $a \in \mathrm{ann}(x_i)$ then $ax_i = 0$ such that $ax_i + M_{i-1} = 0 + M_{i-1}$ and

$$a + \mathfrak{p}_i = a(1 + \mathfrak{p}_i) = a\,\Phi_i(x_i + M_{i-1}) = \Phi_i(ax_i + M_{i-1}) = \Phi_i(0 + M_{i-1}) = 0 + \mathfrak{p}_i$$

such that $a \in \mathfrak{p}_i$. As $a \in \operatorname{ann}(x_i)$ has been arbitrary, this means $\operatorname{ann}(x_i) \subseteq \mathfrak{p}_i$ and thereby $\mathfrak{p}_i \in \operatorname{Supp}(M)$ according to the definition of the support of M.

- In the last step we will prove that the x_i constructed in the step before generate M. In particular this means $\operatorname{rank}(M) \leq n$. So consider any $y \in M = M_n$. Then $\Phi_n(y + M_{n-1}) = a_n + \mathfrak{p}_n$ for some $a_n \in R$. Then we define $y_{n-1} := y - a_n x_n$ and find that

$$\Phi_n\left(y_{n-1} + M_{n-1}\right) \;=\; \Phi_n\left(y + M_{n-1}\right) - a_n \Phi_n\left(x_n + M_{n-1}\right) \;=\; \left(a_n + \mathfrak{p}_n\right) - a_n\left(1 + \mathfrak{p}_n\right) \;=\; 0 + \mathfrak{p}_n$$

 In particular we have $y_{n-1} + M_{n-1} = 0 + M_{n-1}$ which is $y_{n-1} \in M_{n-1}$. Continuing that way we recursively construct $y_k \in M_k$ (where $k \geq j$) and $a_k \in R$ (where $k \geq j+1$) such that $y_{k-1} := y_k - a_k x_k$. Then we continue with picking up any $a_j \in R$ such that $\Phi_j(y_j + M_{j-1}) = a_j + \mathfrak{p}_j$ and let $y_{j-1} := y_j - a_j x_j$ again. We then conclude $y_{j-1} \in M_{j-1}$ in exactly the same way, as for $j = n$. In particular $y_0 \in M_0 = 0$ such that $0 = y_1 - a_1 x_1$. That is we end up with $y_1 = a_1 x_1$ and now work our way up again: We claim that $y_j = a_1 y_1 + \cdots + a_j + x_j$ and proceed inductively: From $y_{j-1} := y_j - a_j x_j$ we get $y_j = y_{j-1} + a_j x_j$ and by induction hypothesis $y_{j-1} = a_1 y_1 + \cdots + a_{j-1} + x_{j-1}$ that's it already. In the end we get $y = y_n = a_1 y_1 + \cdots + a_n x_n$ and as $y \in M$ has been arbitrary, this finishes $M \subseteq \operatorname{Lh}\{ x_1, \ldots, x_n \} \subseteq M$.

□

Proof of (5.16):

(i) We start with (a) $\implies$ (b): By (5.8.(vii)) $\operatorname{zd}(M)$ is the grand union of $\operatorname{Sann}(M)$ and by (5.14) this is a finite set. That is $\mathfrak{a}$ is contained in a union of finitely many prime ideals. By prime avoidance (2.14.(iii)) we find that $\mathfrak{a}$ already is contained in one of them and this is (b).

So for (b) $\implies$ (c): Let $\mathfrak{p} = \operatorname{ann}(x)$ for some $x \neq 0$. Then $\mathfrak{a} \subseteq \mathfrak{p} = \{ a \in R \mid ax = 0 \}$ translates into: For all $a \in \mathfrak{a}$ we have $ax = 0$ and hence $\mathfrak{a}x = \{0\}$, which is (c).

Of course (c) $\implies$ (d) is trivial so we close the circle, proving (d) $\implies$ (a): By assumption for any $a \in \mathfrak{a}$ there is some $x \neq 0$ such that $a \in \operatorname{ann}(x) \in \operatorname{Anns}(M)$. That is $\mathfrak{a}$ is contained in the grand union of $\operatorname{Anns}(M)$. But by (5.7.(iii)) this is $\operatorname{zd}(M)$ already.

(ii) Let us first prove (a) $\implies$ (b): By assumption for any $\mathfrak{p} \in \operatorname{Sann}(M)$ we have $\mathfrak{a} \subseteq \mathfrak{p}$ such that $\mathfrak{p} \in \mathbb{V}(\mathfrak{a})$. Conversely (b) $\implies$ (a): Any $\mathfrak{p} \in \operatorname{Sann}(M)$ is contained in $\mathbb{V}(\mathfrak{a})$ such that $\mathfrak{a} \subseteq \mathfrak{p}$. As this is true for any $\mathfrak{p} \in \operatorname{Sann}(M)$ we conclude that $\mathfrak{a}$ is contained in the grand intersection of $\operatorname{Sann}(M)$. It remains to verify (a) $\iff$ (c): By (5.13) the grand intersection of $\operatorname{Sann}(M)$ is the same, as the grand intersection of $\operatorname{Supp}(M)$. Thus by the same reasoning as for $\operatorname{Sann}(M)$ we find

$$\mathfrak{a} \;\subseteq\; \bigcap \operatorname{Supp}(M) \;=\; \bigcap \operatorname{Sann}(M) \quad\iff\quad \operatorname{Supp}(M) \;\subseteq\; \mathbb{V}(\mathfrak{a})$$

But for $\operatorname{Supp}(M)$ we have shown the equivalence of $\operatorname{Supp}(M) \subseteq \mathbb{V}(\mathfrak{a})$ and (c) in (3.139.(vii)) already. Combining these equivalences we conclude that (a) is equivalent to (c), too

$$\operatorname{Supp}(M) \;\subseteq\; \mathbb{V}(\mathfrak{a}) \quad\iff\quad \exists\, n \in \mathbb{N} \;:\; \mathfrak{a}^n M = 0$$

(iii) The proof will feature two,t he first loop goes like (a) $\implies$ (c) $\implies$ (b) $\implies$ (a) and the second loop like (e) $\implies$ (d) $\implies$ (c) $\implies$ (e). As the loops are interlocked in (c) this grants the

equivalence. We start with (a) $\implies$ (c): Given $a \in R$ let us distinguish two cases: If $a \in \mathfrak{p}$, then $Ra \subseteq \mathfrak{p} = \bigcap \mathrm{Sann}(M)$ such that by (ii) there is some $n \in \mathbb{N}$ such that $(Ra)^n M = 0$. But clearly $(Ra)^n = Ra^n$ and $0 = Ra^n M = a^n M = \mathrm{im}(\lambda_a^n)$. In particular λ_a is nilpotent. And in case $a \notin \mathfrak{p}$ then we use (5.8.(vii)) to find $a \notin \mathfrak{p} = \bigcup \mathrm{Sann}(M) = \mathrm{zd}(M)$ which means $a \in \mathrm{nzd}(M)$. That is $ax = 0$ implies $x = 0$ and hence $\mathrm{kn}(\lambda_a) = 0$, which is the injectivity of λ_a. The most difficult part (c) $\implies$ (b) comes next: Let us denote the following subset of R

$$\mathfrak{p} \;:=\; \{\, a \in R \mid \exists\, n \in \mathbb{N} : a^n M = 0 \,\}$$

Note that $a^n M = 0$ is equivalent to $\lambda_a^n = 0$ such that $a \in \mathfrak{p}$ is equivalent to λ_a being nilpotent. In a first step we will prove, that $\mathfrak{p}$ is an ideal of R. Clearly $0 \in \mathfrak{p}$ by taking $n = 1$. Also if $b \in \mathfrak{p}$ and $a \in R$, then there is some $n \in \mathbb{N}$ such that $b^n M = 0$. But then $(ab)^n M = b^n a^n M \subseteq b^n M = 0$ such that $ab \in \mathfrak{p}$, as well. And if now a, $b \in \mathfrak{p}$, then we have $a^m M = 0$ and $b^n M = 0$ for some m, $n \in \mathbb{N}$. The binomial rule enables us to rewrite

$$\begin{aligned}(a+b)^{m+n} &= \sum_{k=0}^{m+n} \binom{m+n}{k} a^k b^{m+n-k} \\ &= b^n \sum_{k=0}^{m} \binom{m+n}{k} a^k b^{m-k} + a^m \sum_{k=m+1}^{m+n} \binom{m+n}{k} a^{k-m} b^{m+n-k}\end{aligned}$$

Thereby $(a+b)^{m+n} M \subseteq b^n M + a^m M = 0$ such that $a + b \in \mathfrak{p}$ again. Altogether, we have found $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$. Next we verify that (c) makes this ideal a prime ideal: Consider a, $b \in R$ such that $ab \in \mathfrak{p}$. If we had $a \notin \mathfrak{p}$ and $b \notin \mathfrak{p}$ then by assumption (c) both, λ_a and λ_b would be injective. But then $\lambda_{ab} = \lambda_a \lambda_b$ would be injective, too. And this contradicts $ab \in \mathfrak{p}$ (i.e. λ_{ab} being nilpotent). Hence we have $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$ which is the prime property of $\mathfrak{p}$.

It remains to prove $\sqrt{\mathrm{ann}(x)} = \mathfrak{p}$ for any $x \in M$ with $x \neq 0$. Hereby $\mathrm{ann}(x) = \{\, a \in R \mid ax = 0 \,\}$. If $a \in \mathfrak{p}$ then there is some $n \in \mathbb{N}$ such that $a^n M = 0$. In particular $a^n x = 0$ which is $a^n \in \mathrm{ann}(x)$ which turns into $a \in \sqrt{\mathrm{ann}(x)}$. That is we have shown $\mathfrak{p} \subseteq \sqrt{\mathrm{ann}(x)}$. Conversely, if $a \in \mathrm{ann}(x)$, then λ_a is not injective and hence λ_a has to be nilpotent, by (c). That is there is some $n \in \mathbb{N}$ such that $\lambda_a^n = 0$, in other words $0 = \mathrm{im}(\lambda_a^n) = a^n M$. But this is $a \in \mathfrak{p}$ such that we have $\mathrm{ann}(x) \subseteq \mathfrak{p}$. As $\mathfrak{p}$ is prime we find $\sqrt{\mathrm{ann}(x)} \subseteq \sqrt{\mathfrak{p}} = \mathfrak{p}$. Altogether $\sqrt{\mathrm{ann}(x)} = \mathfrak{p}$.

We close the first loop, by proving (b) $\implies$ (a), but this is easy: Consider any $\mathfrak{q} \in \mathrm{Sann}(M)$, in particular $\mathfrak{q} = \mathrm{ann}(x)$ for some $x \neq 0$. As $\mathfrak{q}$ is prime we have $\mathfrak{q} = \sqrt{\mathfrak{q}} = \sqrt{\mathrm{ann}(x)} = \mathfrak{p}$. That is $\mathrm{Sann}(M) \subseteq \{\, \mathfrak{p} \,\}$. But as R is noetherian and M is finitely generated we use (5.8.(vi)) once more to find $\mathrm{Sann}(M) \neq \emptyset$. Thereby we gain (a).

This has been the hard part, the second loop is far easier: We take the back door and begin with (e) $\implies$ (d): We distinguish two cases again, if $a \notin \mathrm{zd}(M)$, then by assumption (e) there is some $x \in M$ such that for any $n \in \mathbb{N}$ we have $a^n x \neq 0$. In particular $a^n M = 0$ is false for all $n \in \mathbb{N}$. In the second case we consider $a \in \mathrm{zd}(M)$, then by (e) given $x \in M$ we find some $n \in \mathbb{N}$, such that $a^n x = 0$. We have required M to finitely generated, say $M = \mathrm{Lh}\{\, x_1, \ldots, x_r \,\}$. Then for any $i \in 1 \ldots r$ we may pick up $n(i) \in \mathbb{N}$, such that $a^{n(i)} x_i = 0$. And if we let $n := \max\{\, n(1), \ldots, n(r) \,\}$ we get $a^n x_i = 0$ for any $i \in 1 \ldots r$. But as the x_i generate M we conclude $a^n M = 0$, which was required by (d).

The implication (d) $\implies$ (c) is trivial: $\mathrm{zd}(M) = \{\, a \in R \mid \exists\, x \in M \,:\, x \neq 0 \text{ and } ax = 0 \,\}$. So suppose λ_a is *not* injective, then $\mathrm{kn}(\lambda_a) \neq 0$, i.e. there is some $x \in M$ with $x \neq 0$ and $ax = 0$. But this means $a \in \mathrm{zd}(M)$. Then by assumption (d) there is some $n \in \mathbb{N}$ such that $a^n M = 0$. This of course is nothing but $\lambda_a^n = 0$, so λ_a either is injective or nilpotent.

It remains to verify (c) $\implies$ (e): Consider any $a \in R$, if λ_a is injective, then $ax = 0$ implies $x = 0$ which is $a \notin \mathrm{zd}(M)$. So suppose for all $x \in M$ there was some $n \in \mathbb{N}$, such that $a^n x = 0$. Choose any $x \neq 0$ and let m be the minimal power, such that $a^m x = 0$. In particular $m \geq 1$ and $a^{m-1}x \neq 0$. Then $\lambda_a(a^{m-1}x) = a^m x = 0$, which contradicts λ_a being injective. That is both sides of the equivalence in (e) are false. If λ_a is nilpotent, then there is some $n \in \mathbb{N}$ such that $a^n M = \mathrm{im}(\lambda_a^n) = 0$. In particular for any $x \in M$ we get $a^n x = 0$. With the same reasoning, as before we find some $y = a^{m-1}x \neq 0$ with $ay = 0$. That is $a \in \mathrm{zd}(M)$ and hence both sides of the equivalence in (e) are true.

□

Proof of (5.18):
Let us first assume, that $\mathfrak{a}$ is a primary ideal, then $\mathfrak{p}$ is a prime ideal, due to (2.90.(ii)). Now, for any $a \in R$ we regard the homothety

$$\lambda_a \,:\, {}^{R}\!\Big/_{\mathfrak{a}} \to {}^{R}\!\Big/_{\mathfrak{a}} \,:\, b + \mathfrak{a} \mapsto ab + \mathfrak{a}$$

We will prove that λ_a either is injective or nilpotent. If λ_a is injective, we are done. Else there is some $b + \mathfrak{a} \neq 0 + \mathfrak{a}$ such that $ab + \mathfrak{a} = 0 + \mathfrak{a}$. That is $b \notin \mathfrak{a}$, but $ab \in \mathfrak{a}$. As $\mathfrak{a}$ is a primary ideal, by (a), there is some $n \in \mathbb{N}$ such that $a^n \in \mathfrak{a}$. Therefore $a^n(1 + \mathfrak{a}) = 0 + \mathfrak{a}$ such that $\lambda_a^n = 0$, that is λ_n is nilpontent. This is property (c) in (5.16.(iii)). Thereby $\mathrm{Sann}(R/\mathfrak{a}) = \{\, \mathfrak{p} \,\}$, where $\mathfrak{p} = \{\, a \in R \mid \exists\, n \in \mathbb{N} : a^n(1 + \mathfrak{a}) = 0 \,\}$ which is $\mathfrak{p} = \{\, a \in R \mid \exists\, n \in \mathbb{N} : a^n \in \mathfrak{a} \,\} = \sqrt{\mathfrak{a}}$.
Conversely suppose $\mathrm{Sann}(R/\mathfrak{a}) = \{\, \mathfrak{p} \,\}$ for $\mathfrak{p} = \sqrt{\mathfrak{a}}$, then we need to show that $\mathfrak{a}$ is a primary ideal. That is we consider a, $b \in R$ with $ab \in \mathfrak{a}$ but $b \notin \mathfrak{a}$ and need to show $a \in \sqrt{\mathfrak{a}} = \mathfrak{p}$. But as $b \notin \mathfrak{a}$ we have $x = b + \mathfrak{a} \neq 0$ and hence by property (b) in (5.16.(iii)) we find $\sqrt{\mathrm{ann}(x)} = \mathfrak{p}$. Yet $ab \in \mathfrak{a}$ implies $ax = a(b + \mathfrak{a}) = 0$ such that $a \in \mathrm{ann}(x)$, in particular $a \in \mathfrak{p}$. □

Proof of (5.20):

(i) As R is noetherian and M is finitely generated, M is noetherian again. Hence $P \leq_{\mathsf{m}} M$ is finitely generated and $P \neq 0$ by assumption, such that $\mathrm{Sann}(P) \neq \emptyset$, according to (5.8.(vi)). But by (5.7.(i)) we also have $\mathrm{Sann}(P) \subseteq \mathrm{Sann}(M) = \{\, \mathfrak{p} \,\}$. Together this can only mean $\mathrm{Sann}(P) = \{\, \mathfrak{p} \,\}$.

(ii) Let us abbreviate $P := P_1 + \cdots + P_n \leq_{\mathsf{m}} M$, then we use (5.8.(ii)) on P to find that the set of associated primes of P is just $\{\, \mathfrak{p} \,\}$ again

$$\mathrm{Sann}(P) \;=\; \bigcup_{k=1}^{n} \mathrm{Sann}(P_k) \;=\; \bigcup_{k=1}^{n} \{\, \mathfrak{p} \,\} \;=\; \{\, \mathfrak{p} \,\}$$

(iii) By assumption any M/P_k is $\mathfrak{p}$-primary (for $k \in 1 \ldots n$). But from (5.8.(iv)) we hence find that the

direct sum of this residue modules is $\mathfrak{p}$-primary, too

$$\mathrm{Sann}\left(\bigoplus_{k=1}^{n} M\Big/_{P_k}\right) \;=\; \bigcup_{k=1}^{n} \mathrm{Sann}\left(M\Big/_{P_k}\right) \;=\; \bigcup_{k=1}^{n} \{\,\mathfrak{p}\,\} \;=\; \{\,\mathfrak{p}\,\}$$

Let us abbreviate $P = P_1 \cap \cdots \cap P_n$ the intersection of the P_k, then there is a monomorphsim of R-modules of the following form

$$M\Big/_{P} \;\hookrightarrow\; \bigoplus_{k=1}^{n} M\Big/_{P_k} \;:\; x+P \mapsto (x+P_k)$$

From this (5.7.(i)) implies $\mathrm{Sann}(M/P) \subseteq \{\,\mathfrak{p}\,\}$. But as M is finitely generated, so is M/P. And as $\mathrm{Sann}(M/P_1) \neq \emptyset$ there is some $x \in M$ with $x+P_1 \neq 0+P_1$. In particular $x \notin P$ such that $M/P \neq 0$, as well. As R is noetherian we get $\mathrm{Sann}(M/P) \neq \emptyset$ from (5.8.(vi)) again. And this can only be $\mathrm{Sann}(M/P) = \{\,\mathfrak{p}\,\}$.

(iv) If L and N are $\mathfrak{p}$-primary we find $\mathrm{Sann}(M) = \{\,\mathfrak{p}\,\}$, as well, since (5.8.(i)) applied to the chain $0 \to L \to M \to N \to 0$ already reads as

$$\{\,\mathfrak{p}\,\} \;=\; \mathrm{Sann}(L) \;\subseteq\; \mathrm{Sann}(M) \;\subseteq\; \mathrm{Sann}(L) \cup \mathrm{Sann}(N) \;=\; \{\,\mathfrak{p}\,\} \cup \{\,\mathfrak{p}\,\} \;=\; \{\,\mathfrak{p}\,\}$$

□

Proof of (5.22):

(i) As M is finitely generated, so is M/P. This together with R being noetherian (5.8.(iv)) implies that $\mathrm{Sann}_{(}M/P) \neq \emptyset$. It remains to prove, that there only is one associated prime of M/P: Hence we consider any two $\mathfrak{p}$, $\mathfrak{q} \in \mathrm{Sann}(M/P)$, say $\mathfrak{p} = \mathrm{ann}(x+P)$ and $\mathfrak{q} = \mathrm{ann}(y+P)$. Then we let $U := Rx+P$ and $V := Ry+P$. As $x+P \neq 0+P$ we have $x \in U$ but $x \notin P$ such that $P \subset U$. Likewise we have $P \subset V$ (as $y \in V \setminus P$) and clearly

$$P \;\subseteq\; U \cap V$$

As P is irreducible, by assumption, and $U, V \neq P$ this means $P \subset U \cap V$ and hence we may choose any $z \in U \cap V$ with $z \notin P$. That is $z+P \in U/P = (Rx+P)/U$ is of the form $z+P = ax+P$ for some $a \in R$. Suppose we had $a \in \mathfrak{p} = \mathrm{ann}(x+P)$, then $z+P = ax+P = a(x+P) = 0+P$ in contradiction, to $z \notin P$. Thus $a \notin \mathfrak{p} = \mathrm{ann}(x+P)$ and as $\mathfrak{p}$ is prime (3.24.(ii)) implies

$$\mathrm{ann}(z+P) \;=\; \mathrm{ann}(ax+P) \;=\; \mathrm{ann}(x+P) \;=\; \mathfrak{p}$$

In complete analogy we find $\mathrm{ann}(z+P) = \mathrm{ann}(y+P) = \mathfrak{q}$ such that both $\mathfrak{p}$ and $\mathfrak{q}$ equal $\mathrm{ann}(z+P)$. In particular $\mathfrak{p} = \mathfrak{q}$. That is $\mathrm{Sann}(M/P)$ is non-empty, but all its elements are identical, meaning it only contains a single element.

(ii) Consider the set of all sub-modules of R, that do *not* have an irreducible decomposition. We claim that this set is empty. Suppose this was not the case, i.e. there was a sub-module that has no irreducible decomposition. As M is a noetherian module, there then would be a *maximal* element

in this set. Let $N \leq_{\mathsf{m}} M$ be such a sub-module, that is maximal among the sub-modules of M without irreducible decomposition.

In particular N cannot be irreducibe itself, as then $P_1 = N$ would be an irreducible decomposition. Therefore there are sub-modules P, $Q \leq_{\mathsf{m}} M$ such that $N = P \cap Q$ but $P \neq N$ and $Q \neq N$. Therefore we have $N \subset P$ and $N \subset Q$. But by maximality of N this means that P and Q *do* have an irreducible decomposition, say $P = P_1 \cap \cdots \cap P_r$ and $Q = Q_1 \cap \cdots \cap Q_s$. But then N

$$N \;=\; P \cap Q \;=\; P_1 \cap \cdots \cap P_r \cap Q_1 \cap \cdots \cap Q_s$$

also has an irreducible decomposition. This clearly is a contradiction that can only be evaded, if there is no sub-module of M that does not have an irreducible decomposition, in the first place.

(iii) Pick up an irreducible decomposition $L = Q_1 \cap \cdots \cap Q_n$ of L, which exists, according to (ii). We may scratch all Q_i from this list that are not really required for L. That is we may assume this decomposition to be minimal in the sense, that for any $i \in 1 \ldots n$ we get

$$L \;\subset\; \bigcap_{i \neq j} Q_i$$

Next we note that due to (i) any Q_i is coprimary in M, that is for any $i \in 1 \ldots n$ there is some $\mathfrak{q}_i \in \operatorname{Spec}(R)$ such that $\operatorname{Sann}(M/Q_i) = \{ \mathfrak{q}_i \}$. Now, for any $\mathfrak{p} \in \operatorname{Spec}(R)$, we may define

$$\begin{aligned} I(\mathfrak{p}) &:= \{ i \in 1 \ldots n \mid \mathfrak{q}_i = \mathfrak{p} \} \\ \mathcal{S} &:= \{ \mathfrak{p} \in \operatorname{Spec}(R) \mid I(\mathfrak{p}) \neq \emptyset \} \end{aligned}$$

That is $\mathcal{S}$ is the set of prime ideals of R, that occur as associated prime ideals of the decomposition Q_i. Clearly $s := \#\mathcal{S} \leq n$ such that $\mathcal{S}$ is finite. Choose an arbitrary numbering $\mathcal{S} = \{ \mathfrak{p}_1, \ldots, \mathfrak{p}_s \}$ of this set, then for any $j \in 1 \ldots s$ we define

$$P_j \;:=\; \bigcap_{i \in I(\mathfrak{p}_j)} Q_i$$

That is P_j is the intersection of all Q_i who belong to the same associated prime ideal $\mathfrak{q}_i = \mathfrak{p}_j$. As such P_j is $\mathfrak{p}_j$-coprimary in M, according to (5.20.(iii)) - this is property (3). And by construction, different P_j have different associated prime ideals $\mathfrak{p}_j$ - that is property (4). Also we have property (1), as we have just rearranged the intersection of the Q_i

$$L \;=\; Q_1 \cap \cdots \cap Q_n \;=\; \bigcap_{j=1}^{s} \bigcap_{i \in I(\mathfrak{p}_j)} Q_i \;=\; \bigcap_{j=1}^{s} P_j$$

But by minimality of the Q_i we also get property (2): For ease of notation say we had $L = P_2 \cap \cdots \cap P_s$, then we would be missing those Q_i that belonged to $\mathfrak{q}_i = \mathfrak{p}_1$, in particular

$$\bigcap_{j \neq 1} P_j \;=\; \bigcap_{\mathfrak{q}_i \neq \mathfrak{p}_1} Q_i \;\supset\; L$$

(iv) Using (3.125.(i)) we find an isomorphy of the $U^{-1}R$-modules $U^{-1}M/U^{-1}P_i$ and $U^{-1}(M/P_i)$. And by (5.12.(ii)) there is a 1:1 correspondence of the associated prime ideals, of the form

$$\begin{aligned}\mathrm{Sann}_{U^{-1}R}\left(U^{-1}M\Big/U^{-1}P_i\right) &= \mathrm{Sann}_{U^{-1}R}\left(U^{-1}\left(M\Big/P_i\right)\right)\\ &\longleftrightarrow \left\{\mathfrak{p}\in\mathrm{Sann}_R\left(M\Big/P_i\right)\mid \mathfrak{p}\cap U=\emptyset\right\}\end{aligned}$$

By assumption (iii) $\mathrm{Sann}(M/P_i)$ contains the single element $\mathfrak{p}_i$, therefore there only are two cases: If $\mathfrak{p}_i\cap U=\emptyset$, then then $U^{-1}M/U^{-1}P_i$ contains the single element $U^{-1}\mathfrak{p}_i$ by (5.12.(ii)). That is: $U^{-1}P_i$ is $U^{-1}\mathfrak{p}_i$-primary in $U^{-1}M$. Alternatively, if $\mathfrak{p}_i\cap U\neq\emptyset$ recall that M/P_i is $\mathfrak{p}_i$-primary. Therefore by (5.16.(iii)) we have $\sqrt{\mathrm{ann}(x+L)}=\mathfrak{p}_i$ for any $x+P_i\neq 0+P_i$. From this we find some $u\in\sqrt{\mathrm{ann}(x+L)}\cap U$, hence there is some power $n\in\mathbb{N}$ such that $u^n\in\mathrm{ann}(x+L)$, which is $u^n(x+L)=0+L=u^n(0+L)$. As U is multiplicatively closed $u^n\in U$, as well, such that $(x+L)/v=(0+L)/1$ for any $v\in U$. And as this is true, for any $v\in U$ and any $x+P_i\neq 0+P_i$ we find $U^{-1}(M/P_i)=0$, in this case. Let us summarize

$$\begin{aligned}\mathfrak{p}_i\cap U=\emptyset &\iff \mathrm{Sann}_{U^{-1}R}\left(U^{-1}M\Big/U^{-1}P_i\right)=\left\{U^{-1}\mathfrak{p}_i\right\}\\ \mathfrak{p}_i\cap U\neq\emptyset &\iff U^{-1}M\Big/U^{-1}P_i=0\end{aligned}$$

In particular this is property (3) of the reduced primary decomposition of $U^{-1}L$. And by (2.129) $\mathfrak{p}\mapsto U^{-1}\mathfrak{p}$ is a 1:1 correspondence between the prime ideals $\mathfrak{p}$ of R with $\mathfrak{p}\cap U=\emptyset$ and the prime ideals of $U^{-1}R$. Therefore, as the $\mathfrak{p}_i$ are pairwise distinct, so are the $U^{-1}\mathfrak{p}_i$ and this also is property (4) of a reduced primary decomposition. Now, as in (3.127) let us denote $k:P\mapsto U^{-1}P$ the surjective map, that turns R-sub-modules of M into $U^{-1}R$-sub-modules of $U^{-1}M$. We have also seen there, that k respects finite intersections, that is

$$k(L)=k\left(\bigcap_{i=1}^{s}P_i\right)=\bigcap_{i=1}^{s}k(P_i)$$

But as we have argued above, whenever $\mathfrak{p}_i\cap U\neq\emptyset$ we have $U^{-1}M/U^{-1}P_i=0$ and hence $k(P_i)=U^{-1}P_i=U^{-1}M$, such that these $k(P_i)$ do not contribute to the intersection. That is we find property (1) of reduced primary decompositions

$$U^{-1}L=\bigcap_{\mathfrak{p}_i\cap U=\emptyset}U^{-1}P_i$$

It remains to verify property (2): To do this we prove that for any P_i with $\mathfrak{p}_i\cap U=\emptyset$ we have $\overline{k}k(P_i)=P_i$. As we have seen in (3.127) it suffices to show the following: Consider any $x\in M$ and any $u\in X$ such that $ux\in P_i$, then we have to show $x\in P_i$. Now $ux\in P_i$ means $u\in\mathrm{ann}(x+P_i)$ and as before we have $\mathrm{ann}(x+P_i)\subseteq\sqrt{\mathrm{ann}(x+P_i)}=\mathfrak{p}_i$ which is $u\in\mathfrak{p}_i$ such that $u\in\mathfrak{p}_i\cap U=\emptyset$. From this contradiction we conclude $\overline{k}k(P_i)=P_i$.

For ease of notation say the sub-modules with $\mathfrak{p}_i\cap U=\emptyset$ are $U^{-1}P_i$ where $i\in 1\ldots r$ and for

$r < i \leq s$ we have $U^{-1}P_i = U^{-1}M$. Property (3) of reduced primary decompositions then reads as

$$\forall\, j \in 1 \ldots r \quad : \quad \bigcap_{i \neq j} U^{-1}P_i \;\neq\; U^{-1}L$$

By symmetry of the argument it suffices to regard the case $j = 1$. $U^{-1}P_2 \cap \cdots \cap U^{-1}P_r = U^{-1}L$ is equivalent to $U^{-1}P_2 \cap \cdots \cap U^{-1}P_r \subseteq U^{-1}P_1$ according to (0.1). But as for any $i \in 1 \ldots r$ we have $\bar{k}k(P_i) = P_i$ and $\bar{k}$ respects intersections we would then get

$$P_2 \cap \cdots \cap P_r \;=\; \bar{k}k(P_2) \cap \cdots \cap \bar{k}k(P_2) \;=\; \bar{k}\,(k(P_2) \cap \cdots \cap k(P_r)) \;\subseteq\; \bar{k}k(P_r) \;=\; P_r$$

This again is equivalent to $P_1 \cap \cdots \cap P_r = P_2 \cap \cdots \cap P_r$. But then we could omit P_1 in the primary decomposition of $L = P_1 \cap \cdots \cap P_s$. But as this decomposition is reduced, this cannot be. We conclude that the decomposition $U^{-1}L = U^{-1}P_1 \cap \cdots \cap U^{-1}P_r$ satisfies property (2) of reduced primary decompositions, as well.

□

Proof of (5.23):

(i) An $M/L \to M/P_i : x + L \mapsto x + P_i$ is well-defined, as $L \subseteq P_i$. Thus $x + L \mapsto (x + P_i)$ is a well-defined homomorphism of R-modules. But the injectivity is easy to see: If $(x + P_i) = (0 + P_i)$, then for any $i \in 1 \ldots n$ we have $x \in P_i$ such that $x \in P_1 \cap \cdots \cap P_s = L$. Again this is $x + L = 0 + L$.

(ii) Due to (i) and (5.7.(i)) the associated prime spectrum of M/L is contained in the associated prime spectrum of the direct sum of the M/P_i. But by (5.8.(iv)) this is

$$\mathrm{Sann}\left(M\big/_L\right) \;\subseteq\; \mathrm{Sann}\left(\bigoplus_{i=1}^{s} M\big/_{P_i}\right) \;=\; \bigcup_{i=1}^{s} \mathrm{Sann}\left(M\big/_{P_i}\right) \;=\; \bigcup_{i=1}^{s} \{\,\mathfrak{p}_i\,\}$$

Thus we have $\mathrm{Sann}(M/L) \subseteq \{\,\mathfrak{p}_1, \ldots, \mathfrak{p}_s\,\}$. For the converse inclusion we prove $\mathfrak{p}_1 \in \mathrm{Sann}(M/L)$. Due to the symmetry of the argument this does suffice. To do this regard

$$\varphi \;:\; P_2 \cap \cdots \cap P_s\big/_L \to M\big/_{P_1} \;:\; x + L \mapsto x + P_i$$

As $L \subseteq P_1$ this is a well-defined R-module homomorphism. And given $x \in P_2 \cap \cdots \cap P_s$ with $x + P_1 = 0 + P_1$ we had $x \in P_1$ as well, such that $x \in P_1 \cap (P_2 \cap \cdots \cap P_s) = L$. Thus $x + L = 0 + L$, which is the injectivity of φ. Yet, as the P_i are a *reduced* decomposition of L, we have $L \subset P_2 \cap \ldots P_s$ that is there is some $x \in P_2 \cap \ldots P_s$ with $x \notin L$. Therefore $(P_2 \cap \ldots P_s)/L \neq 0$ is not the zero-module. Thus by (5.8.(vi)) $\mathrm{Sann}((P_2 \cap \ldots P_s)/L) \neq \emptyset$, yet as φ is injective

$$\emptyset \;\neq\; \mathrm{Sann}\left(P_2 \cap \cdots \cap P_s\big/_L\right) \;\subseteq\; \mathrm{Sann}\left(M\big/_{P_1}\right) \;=\; \{\,\mathfrak{p}_1\,\}$$

such that we conclude $\mathrm{Sann}((P_2 \cap \cdots \cap P_s)/L) = \{\,\mathfrak{p}_1\,\}$ once more. But as $(P_2 \cap \cdots \cap P_s)/L$ is a sub-module of M/L this implies $\mathfrak{p}_1 \in \mathrm{Sann}(M/L)$, too - all by (5.7.(i)) - and as we could have done this with any $i \in 1 \ldots s$ we see $\{\,\mathfrak{p}_1, \ldots, \mathfrak{p}_s\,\} \subseteq \mathrm{Sann}(M/L)$, as well.

(iii) Suppose $\mathfrak{p}_k$ is minimal and take $U := R \setminus \mathfrak{p}_k$. Suppose we have $\mathfrak{p}_i \cap U = \emptyset$, then we had $\mathfrak{p}_i \subseteq \mathfrak{p}_k$ and as $\mathfrak{p}_k$ is minimal, this is $\mathfrak{p}_i = \mathfrak{p}_k$. Now, as the $\mathfrak{p}_i$ are pairwise distinct, this implies $i = k$. Thus

we have $\mathfrak{p}_i \cap U = \emptyset$ is and only if $i = k$. By (5.22.(iv)) we have a reduced primary decomposition of $U^{-1}L$, given by

$$\left\{ U^{-1}P_i \mid i \in 1 \ldots s, \mathfrak{p}_i \cap U = \emptyset \right\} \;=\; \left\{ U^{-1}P_k \right\}$$

In particular $U^{-1}L = U^{-1}P_k$ (considered, as subsets of $U^{-1}M$). Also we have seen there, that P_k is $\kappa^{-1}(U^{-1}P_k) = \kappa^{-1}(U^{-1}L)$ - in the proof of (5.22.(iv)) we have used the notation $P_k = \bar{k}k(L)$. But by (3.127) this already is given, to be

$$P_k \;=\; \bar{k}k(L) \;=\; \{ x \in M \mid \exists\, u \in U \,:\, ux \in L \}$$

We could end here, as in particular P_k is uniquely determined by L, but in literature this usually is given as the kernel of $x + L \mapsto (x + L)/1$. So when do we get $(x + L)/1 = (0 + L)/1$? Clearly iff there is some $u \in U$ such that $u(x + L) = u(0 + L) = 0 + L$, which is $ux \in L$. And this is precisely the condition in the set $\bar{k}k(L)$ above.

□

Proof of (5.26):
Item (i) is purely definitional, there is nothing to prove. In (ii) we claim that for an integral domain R the hull $\mathrm{Hull}(P)$ is a sub-module of M again: Thus consider $x, y \in \mathrm{Hull}(P)$ and $r \in R$. By definition there are some $a, b \in R$ such that $a, b \neq 0$ and $ax \in P$ and $by \in P$. But then $a(rx) = r(ax) \in P$ again, such that $rx \in \mathrm{Hull}(P)$, as well. And $(ab)(x + y) = b(ax) + a(by) \in P$ is plain, as well. As $a, b \neq 0$ and R is an integral domain we have $ab \neq 0$ and thereby $x + y \in \mathrm{Hull}(P)$ again. If $p \in P$, then $1p \in P$ and as R is an integral domain we have $1 \neq 0$. Therefore we have the inclusion $P \subseteq \mathrm{Hull}(P)$. Now if $x \in \mathrm{tor}(M)$ is a torsion element, then by definition there is some $a \in R$ with $a \neq 0$ such that $ax = 0 \in P$. Thus we also have $\mathrm{tor}(M) \subseteq \mathrm{Hull}(P)$. And as $\mathrm{Hull}(P)$ is a sub-module this implies $P + \mathrm{tor}(M) \subseteq \mathrm{Hull}(P)$.

In item (iii) we have to check the well-definedness of the content: First of all - as $M \neq 0$ the basis is non-empty $I \neq \emptyset$ and thus we may apply the greatest common divisor. So let us check the independence of the basis: If $\{ m_i \mid i \in I \}$ is a basis with $x = \sum_i a_i m_i$ and $\{ n_i \mid i \in I \}$ is a basis with $x = \sum_i b_i n_i$ then let us denote $A := \{ a_i \mid i \in I \}$ and $B := \{ b_i \mid i \in I \}$ respectively. We need to verify that $\gcd(A) = \gcd(B)$. To do this let

$$m_i \;=\; \sum_{j \in I} a_{i,j} n_j$$

for any $i \in I$. If now $c \in \gcd(A)$ and $d \in \gcd(B)$, in particular $c \mid a_i$ for any $i \in I$. Then we have $a_i = ca'_i$ for some $a'_i \in R$ and thereby

$$x \;=\; \sum_{i \in I} a_i m_i \;=\; \sum_{i \in I} ca'_i \sum_{j \in I} a_{i,j} n_j \;=\; \sum_{j \in I} c \left(\sum_{i \in I} a'_i a_{i,j} \right) n_j$$

As the n_j form a basis we can compare coefficients to find $b_j = c \sum_i a'_i a_{i,j}$ such that $c \mid b_j$ for any $j \in I$. This is $c \mid B$ and as d is a greatest common divisor of B this implies $c \mid d$. In complete analogy we find $d \mid c$ such that c and d are associate $c \approx d$. This again implies

$$\gcd(A) \;=\; cR^* \;=\; dR^* \;=\; \gcd(B)$$

□

Proof of (5.28):

(i) Let us start with $x_0 := x$ and $a_0 := 1$. We will recursively construct $x_n \in M$ and $a_n \in R$ such that $x = a_n x_n$, $\operatorname{ann}(x_n) = 0$ and

$$Rx_0 \subset Rx_1 \subset \ldots \subset Rx_n$$

For $n = 0$ everything is granted, so suppose we already have x_n and a_n. If x_n is primitive, then we are done, as we can take $p := x_n$ and $a := a_n$. If x_n is not primitive, then there are some $b \in R$ and $y \in M$ such that $x_n = by$ and $b \notin R^*$. We will now prove that $Rx_n \subset Ry$: First of all $ax_n = aby \in Ry$ such that $Rx_n \subseteq Ry$ is clear. And since $\operatorname{ann}(x_n) = 0$ we also have $\operatorname{ann}(y) = 0$: If we have $ay = 0$ then $ax_n = aby = bay = b0 = 0$ such that $a = 0$. Suppose we even had the equality $Rx_n = Ry$, then $y \in Rx_n$ would mean $y = ax_n = aby$ for some $a \in R$. But this is $(1 - ab)y = 0$ and thereby $1 - ab = 0$, as $\operatorname{ann}(y) = 0$. But $1 = ab$ would imply $b \in R^*$ which is untrue. Thus we have $y \notin Rx_n$ and thereby $Rx_n \subset Ry$. Now we may take $x_{n+1} := y$ and $a_{n+1} := a_n b$ then $a_{n+1}x_{n+1} = a_n by = a_n x_n = x$.

Thus we have seen: If x_n is not primitive, then we may append the strictly increasing chain $Rx_0 \subset Rx_1 \subset \ldots \subset Rx_n$ by another link $Rx_n \subset Rx_{n+1}$. But as M is noetherian there is no infinitely ascending chain of sumbodules, so this has to stop at some point $m \in \mathbb{N}$. But this only is the case if x_m is primitive and $x = a_m x_m$.

(ii) Let $\{ m_i \mid i \in I \}$ be a basis of M and let $A := \{ a_i \mid i \in I \} \subseteq R$ be the coefficients of the basis representation of x, that is

$$x = \sum_{i \in I} a_i m_i$$

If $c \in \operatorname{cont}(x) = \gcd(A)$ then for any $i \in I$ there is some $a_i' \in R$ such that $a_i = ca_i'$ and thereby we find x in the form

$$x = cp \quad \text{where} \quad p = \sum_{i \in I} a_i' m_i$$

We will now prove $1 \in \operatorname{cont}(x) \implies x$ primitive: We have to regard $b \in R$ and $y \in M$ such that $x = by$. Writing $y = \sum_i b_i m_i$ we find

$$\sum_{i \in I} a_i m_i = x = by = \sum_{i \in I} bb_i\, m_i$$

such that $a_i = bb_i$ for any $i \in I$ by comparing coefficients. In particular $b \mid A$ such that $b \mid c = \gcd(A)$. But as $1 \in \operatorname{cont}(x) = cR^*$ we have $c \in R^*$ and then $b \mid c$ implies $b \in R^*$ such that x truly is primitive. As $1 \in \operatorname{cont}(p)$ by construction this already implies that p is primitive. Conversely for x primitive $\implies 1 \in \operatorname{cont}(x)$ we may use $x = cp$ to find $c \in R^*$ and hence $1 \in cR^* = \operatorname{cont}(x)$.

(iii) We will distinguish several cases: First of all, if $\dim(M) = 1$, then there is a basis $\{ y_1 \}$ of M. As $p \in M = Ry_1$ we get $p = ay_1$ for some $a \in R$. But as p is primitive we get $a \in R^*$. And this means $x \mapsto ax$ is an automorphism of M that maps p to y_1. In particular $\{ p \}$ is a basis of M, as well. Next consider the case $\dim(M) = 2$, then there is a basis $\{ y_1, y_2 \}$ of M. As $p \in M = Ry_1 + Ry_2$ there are some $a, b \in R$ such that $p = ay_1 + by_2$. As p is primitive (ii) tells us, that $1 \in \gcd\{ a, b \}$.

That is there are some $u, v \in R$ such that

$$au + bv \;=\; 1$$

Now define $m_1 := p$ and $m_2 := -vy_1 + uy_2$, we will prove that $\{ m_1, m_2 \}$ is a basis of M, starting with $\mathrm{Lh}\{ m_1, m_2 \} = M$:

$$\begin{aligned} up - bm_2 &= u(ay_1 + by_2) - b(-vy_1 + uy_2) \\ &= (au + bv)y_1 + (ub - bu)y_2 \;=\; y_1 \\ vp + am_2 &= v(ay_1 + by_2) + a(-vy_1 + uy_2) \\ &= (va - av)y_2 + (bv + au)y_2 \;=\; y_2 \end{aligned}$$

Thus we have y_1 and $y_2 \in \mathrm{Lh}\{ m_1, m_2 \}$ and as these generate M we already get $M = \mathrm{Lh}\{ m_1, m_2 \}$. That is $\{ m_1, m_2 \}$ generates M. It remains to show, that $\{ m_1, m_2 \}$ also is linearly independent. Thus consider some $c, d \in R$ such that $cm_1 + dm_2 = cp + dm_2 = 0$. That is

$$\begin{aligned} c(ay_1 + by_2) + d(-vy_1 + uy_2) &= 0 \\ (ac - dv)y_1 + (bc + du)y_2 &= 0 \end{aligned}$$

As $\{ y_1, y_2 \}$ is a basis and hence linearly independent we find the following system of linear equations, as the coefficients in front of y_1 and y_2 have to vanish

$$\begin{aligned} ac - dv &= 0 \\ bc + du &= 0 \end{aligned}$$

Multiplying the upper equation with u, the lower with v and then adding the results leads to $0 = acu - duv + bcv + duv = (au + bv)c = c$ and multiplying the upper equation with $-b$, the lower with a and then adding the results leads to $0 = -abc + bdv + abc + adu = (bv + au)d = v$. Thus we found $c = 0$ and $d = 0$ which means that $\{ m_1, m_2 \}$ is a basis of M that contains p, as $p = m_1$.

(iii) Next we consider the case $\dim(M) < \infty$, that is M is finitely generated. Let $n := \dim(M)$, by induction we may assume, that the statement is true for all modules of rank $n - 1$ or lower. So pick up a basis $\{ y_1, \ldots, y_n \}$ of M and define $Q := \mathrm{Lh}\{ y_1, \ldots, y_{n-1} \} \leq_{\mathfrak{m}} M$. Then we clearly have

$$M \;=\; Q \oplus Ry_n$$

Let $p = \sum_i a_i y_i$ be the representation of p in this basis. If $a_n = 0$ then $p \in Q$ and as $\dim(Q) = n - 1 < n$ this would mean there is some basis $\{ m_1, \ldots, m_{n-1} \}$ of Q that contains p. But then $\{ m_1, \ldots, m_{n-1}, y_n \}$ would be a basis of M containing p, which we needed to find. So this case is done and we continue with $a_n \neq 0$. Now let

$$y \;:=\; p - a_n y_n \;=\; \sum_{i=1}^{n-1} a_i y_i \;\in\; Q$$

If $y = 0$, then $p = a_n y_n$ and by the case $n = 1$ above this would mean, that p is a basis of Ry_n. In particular $\{ y_1, \ldots, y_{n-1}, p \}$ would be a basis of M containing p. So this case is done, as well and we continue with $y \neq 0$. Then by (ii) there is some primitive $q \in Q$ such that $y = bq$ where $b = \mathrm{cont}(y) = \gcd\{ a_1, \ldots, a_{n-1} \}$. By induction hypothesis there is a basis $\{ m_1, \ldots, m_{n-1} \}$ of Q containing Q. Without loss of generality we have $q = m_1$. Then $\{ q, m_2, \ldots, m_{n-1}, y_n \}$ is a basis of M and we have

$$M \;=\; \mathrm{Lh}\{ m_2, \ldots, m_{n-1} \} \oplus \mathrm{Lh}\{ q, y_n \}$$

Note that $p = y + a_n y_n = bq + a_n y_n$ is a basis representation of p in that basis. And as p is primitive we therefore have $1 \in \mathrm{cont}(p) = \gcd\{ b, a_n \}$. Let $P := \mathrm{Lh}\{ q, y_n \}$, as p is primitive and $\dim(P) = 2$ the case $n = 2$ above tells us that there is a basis $\{ p, m_n \}$ of P. That is we can exchange $P = \mathrm{Lh}\{ q, y_n \}$ in the above inner direct sum by $\mathrm{Lh}\{ p, m_n \}$ and thereby get a basis $\{ p, m_2, \ldots, m_{n-1}, m_n \}$ of M that contains p. Thus item (iii) is proved for any finitely generated, free module M.

(iii) Now if M is not finitely generated $\dim(M) = \infty$, then we still pick up a basis $\{ y_i \mid i \in I \}$ of M. Then there is a *finite* subset $\Omega \subseteq I$ such that $p \in M$ has the basis representation

$$p \;=\; \sum_{i \in \Omega} a_i y_i$$

Now let $P := \mathrm{Lh}\{ y_i \mid i \in \Omega \}$ and $Q := \mathrm{Lh}\{ y_j \mid j \in I \setminus \Omega \}$, then it is clear that $p \in P$ and $M = P \oplus Q$. As P is finitely generated and free, we already know that there is a basis $\{ m_i \mid i \in \Omega \}$ of P containing p. But then we have found a basis of M containing p, namely

$$p \;\in\; \{ m_i \mid i \in \Omega \} \cup \{ y_j \mid j \in I \setminus \Omega \}$$

(iv) Let $n := \mathrm{rank}(P)$, by assumption P is finitely generated and hence $n \in \mathbb{N}$, such that we can use induction on n. But first of all, if $n = 0$ then $P = 0$ and there is nothing to prove. If $n = 1$, then there is a basis $\{ x \}$ of P and we write $x = dp$ for $d = \mathrm{cont}(p)$ and some primitive $p \in M$. Then by (iii) there is a basis $\{ m_i \mid i \in I \}$ of M that contains $p \in \{ m_i \mid i \in I \}$. Letting $p_1 := p$ and $d_1 := d$ this already is property (1) and property (2) is void in the case $n = 1$. Thus $n = 1$ is complete and we may proceed with $n \geq 2$:

For $n \geq 2$ we start with $M_1 := M$ and $P_1 := P$ and consider the following set $\mathcal{A}$ of ideals in R. Thereby $\mathrm{cont}(x)R$ denotes the ideal generated by $\mathrm{cont}(x) \subseteq R$. Yet if $c \in \mathrm{cont}(x)$ then $\mathrm{cont}(x)R = cR$, as $\mathrm{cont}(x) = cR^* \subseteq cR$. Thus we have $\mathrm{cont}(x)R = \mathrm{cont}(y)R$ if and only if $\mathrm{cont}(x) = \mathrm{cont}(y)$. Now let

$$\mathcal{A} \;:=\; \{ \mathrm{cont}(x)R \mid x \in P,\, x \neq 0 \}$$

Note that R is a PID and hence a noetherian ring such that $\mathcal{A}$ contains a maximal element. Let $x \in P_1 = P$ be an element, such that $dR = \mathrm{cont}(x)R \in \mathcal{A}^*$ is maximal. As $x \neq 0$ we may write $x = dp$ for some primitive $p \in M$ according to (ii). And by (iii) there is a basis $\mathcal{M}_1 := \{ m_j \mid j \in J \}$ of $M_1 = M$ such that $p \in \mathcal{M}_1$. Take $\mathcal{M}_2 := \mathcal{M}_1 \setminus \{ p \}$ and $M_2 := \mathrm{Lh}(\mathcal{M}_2)$. That is: If $p = m_k$

for some $k \in J$ then we have $\mathcal{M}_2 = \{ m_i \mid i \in I \}$ where $I := J \setminus \{ k \}$. Then

$$M_1 \;=\; M \;=\; Rp \oplus M_2$$

Also let $P_2 := P \cap M_2 \;\leq_{\mathsf{m}}\; M_2$. The central part of this proof is to establish the following inner direct sum

$$P_1 \;=\; P \;=\; Rx \oplus P_2$$

First of all we have $x = dp$ and hence $Rx = Rdp \subseteq Rp$. And by also $P_2 \subseteq M_2$ by construction. Therefore we have $Rx \cap P_2 \subseteq Rp \cap M_2 = 0$ such that $Rx \cap P_2 = 0$. So for now we have to prove $P_1 = Rx + P_2$. To do this consider any $y \in P_1$ and use a basis representation of y in terms of $\mathcal{M}_1 = \{ p \} \cup \mathcal{M}_2$:

$$y \;=\; cp + \sum_{i \in I} a_i m_i$$

Let $b \in \gcd\{ c, d \}$, then there are some $u, v \in R$ such that $b = uc + vd$. If $z := ux + vy$ then z has the following representation in $\mathcal{M}_1$

$$\begin{aligned} z \;&=\; ux + vy \;=\; udp + vy \\ &=\; (ud + vc)p + \sum_{i \in I} va_i m_i \;=\; bp + \sum_{i \in I} va_i m_i \end{aligned}$$

As $x \neq 0$ we have $d \neq 0$ and thereby $b \neq 0$ such that $z \neq 0$. Also note that $x \in P_1$ and $y \in P_1$ such that $z \in P_1$. So we have $\mathrm{cont}(z)R \in \mathcal{A}$ by definition of $\mathcal{A}$. But $\mathrm{cont}(z)$ is the greatest common divisor of b and the va_i, so in particular $\mathrm{cont}(z)$ divides b which divides d, that is $Rd \subseteq Rb \subseteq \mathrm{cont}(z)R$. By maximality of Rd in $\mathcal{A}$ this implies $Rd = \mathrm{cont}(z)R$ and thereby $Rd = Rb$. Thus $d \approx b \mid c$ implies $d \mid c$, say $c = dc'$ for some $c' \in R$. That is

$$y \;=\; c'x + \sum_{i \in I} a_i m_i \;\in\; Rx + M_2$$

And as $\sum_i a_i m_i = y - c'x \in P_1$ this is $\sum_i a_i m_i \in P_1 \cap M_2 = P_2$. As y has been arbitrary, this is $P_1 = Rx + P_2$ as desired. Thus we have established the decomposition of P_1 as the inner direct sum.

Now $n = \mathrm{rank}(P_1) = \mathrm{rank}(Rx \oplus P_2) = \mathrm{rank}(Rx) + \mathrm{rank}(P_2) = 1 + \mathrm{rank}(P_2)$ such that $\mathrm{rank}(P_2) = n - 1 < n$. Also $P_2 \;\leq_{\mathsf{m}}\; P_1 = P \;\leq_{\mathsf{m}}\; M_2$ and M_2 is a free R-module. So we may use the induction hypothesis to find a basis $\mathcal{Q} = \{ q_i \mid i \in I \}$ of M_2, a subset $\{ p_2, \ldots, p_n \} \subseteq \mathcal{Q}$ and scalars $\{ d_2, \ldots, d_n \} \subseteq R$ such that $\{ d_i q_i \mid i \in 2 \ldots n \}$ is a basis of P_2 and $d_{i-1} \mid d_i$ for any $i \in 3 \ldots n$. We now let $p_1 := p$ and $d_1 := d$. Then $d_1 p_1 = dp = x$ such that $\{ d_i q_i \mid i \in 1 \ldots n \}$ is a basis of $P_1 = P$. This is property (1) already. For property (2) we still have to show $d_1 \mid d_2$. To see this let $s := d_1 p_1 + d_2 p_2 \in P$. Note that this already is the representation of s in the basis $\mathcal{M}_1$ and thereby $\mathrm{cont}(s)R = \gcd\{ d_1, d_2 \}R$. As $d_1 = d \neq 0$ again, we have $s \neq 0$ such that $\mathrm{cont}(s)R \in \mathcal{A}$. But by construction $\mathrm{cont}(s)$ divides d_1 such that $dR = d_1 R \subseteq \mathrm{cont}(s)R$. By the maximality of dR in $\mathcal{A}$ again, this is $d_1 R = \mathrm{cont}(s)R$ and thereby $d_2 R \subseteq \mathrm{cont}(s)R = d_1 R$ which is $d_1 \mid d_2$. This has been the last piece to fit in and the proof is complete.

□

Proof of (5.31):

(ii) For any $j \in 1 \dots r$ let us denote the generator of the sub-module $R/d_jR \hookrightarrow T$ by t_j. That is t_j is the following element

$$t_j \;:=\; \big(\delta_{i,j} + d_iR\big) \;\in\; T$$

As $d_{i-1} \mid d_i$ for any $i \in 2 \dots r$ it is clear (by induction) that $d_i \mid d_r$ for any $i \in 1 \dots r$. Therefore we have $d_r(1 + d_iR) = d_r + d_iR = 0 + d_iR$ such that $d_r t_i = 0$ for any $i \in 1 \dots r$. As the t_i generate T this means $d_r \in \mathrm{ann}(T)$. If conversely $a \neq 0$ with $at_i = 0$ for any $i \in 1 \dots r$, then in particular $at_r = 0$. But this means $0 + d_rR = a(1 + d_rR) = a + d_rR$ such that $d_r \mid a$. In particular we get $\mathrm{ann}(T) = d_rR$.

(iii) As $d_rT = 0$ and $d_r \neq 0$ it is clear that $0^f \oplus T \subseteq \mathrm{tor}(M)$. Conversely consider any $x \in M$ such that $ax = 0$ for some $a \neq 0$. As any element $x \in M$ is of the form $x = (u, v)$ where $u \in R^f$ and $v \in T$ we in particular have $au = 0$. For $u = (u_1, \dots, u_f) \in R^f$ this means $au_i = 0$ for any $i \in 1 \dots f$. But as $a \neq 0$ and R is an integral domain, this implies $u_i = 0$ such that $u = 0$ and thereby $x = (0, v) \in 0^f \oplus T$.

(i) If we take $F := R^f \oplus 0^r \;\leq_{\mathrm{m}}\; M$ then $M = F \oplus T$. And T is generated by $\{\, t_1, \dots, t_r \,\}$ which we defined in (iii). As $d_it_i = 0$ any set $\{\, t_i \,\}$ is linearly dependent (recall $d_i \neq 0$). In particular $F \cup \{\, t_i \,\}$ is linearly dependent and hence (3.102.(v)) implies that $\mathrm{free}(M) = \dim(F) = f$.

(iv) If $r = 0$ then clearly R^f is free, as it admits the Euclidean basis. If conversely M is free, then M is torsion-free (R is an integral domain) according to (3.23.(ii)). And this implies $T = 0$ such that $r = 0$.

(v) If $f = 0$ then $d_rM = 0$ according to (iii) such that M is a torsion-module. Conversely if M is a torsion module then $M = \mathrm{tor}(M) = 0^f \oplus T$ due to (iv). Comparing this to $M = R^f \oplus T$ we find $f = 0$.

(vi) As $\{\, t_1, \dots, t_r \,\}$ generates T it is clear that $\mathrm{rank}(T) \leq r$. Now suppose $q := \mathrm{rank}(T) < r$, that is there is a set $\{\, g_1, \dots, g_q \,\} \subseteq T$ such that there is an epimorphism of R-modules

$$\gamma \;:\; R^q \;\twoheadrightarrow\; T \;:\; (a_1, \dots, a_q) \;\mapsto\; \sum_{k=1}^{q} a_k q_k$$

In particular for any $i \in 1 \dots r$ there has to be some $u_i \in R^q$ such that $t_i = \gamma(u_i)$. Now regard the following matrix

$$U \;=\; \begin{pmatrix} | & | & & | \\ u_1 & u_2 & \dots & u_r \\ | & | & & | \end{pmatrix} \in \mathrm{mat}_{q,r}(R)$$

Then by (4.72.(i)) we have $\text{c-rank}(U) \leq q < r$ and this means that the columns of U have to be linearly dependent. In particular there are some $a_1, \dots, a_r \in R$ that are not all zero [say $a_j \neq 0$], such that

$$\sum_{i=1}^{r} a_i u_i \;=\; 0$$

We will now prove that in general, that for any $a_1, \ldots, a_r \in R$ we always have the following implication

$$\sum_{i=1}^{r} a_i u_i \;=\; 0 \quad\Longrightarrow\quad \forall\, i \in 1 \ldots r \;:\; d_1 \mid a_i$$

To see this simply compute

$$0 \;=\; \gamma\left(\sum_{i=1}^{r} a_i u_i\right) \;=\; \sum_{i=1}^{r} a_i \gamma(u_i) \;=\; \sum_{i=1}^{r} a_i t_i \;=\; \big(a_i + d_i R\big) \;\in\; T$$

This means $0 + d_i R = a_i + d_i R$ for any $i \in 1 \ldots r$ and thereby $d_i \mid a_i$. But by assumption we have $d_{i-1} \mid d_i$ for any $i \in 2 \ldots r$ such that by induction we find $d_1 \mid d_i$ for any $i \in 1 \ldots r$. Now $d_1 \mid d_i$ and $d_i \mid a_i$ together imply $d_1 \mid a_i$. That is there are some $a'_1, \ldots, a'_r \in R$ such that $d_1 a'_i = a_i$. So we have proved the implication above. But from this we also get

$$0 \;=\; \sum_{i=1}^{r} a_i u_i \;=\; d_1 \left(\sum_{i=1}^{r} a'_i u_i\right)$$

Let us abbreviate $d := d_1$ and recall that $d \neq 0$ by assumption. Then this equation can only hold true, if the sum in brackets is zero. This however enables us to repeat this construction indefinitely however and thereby arrive at a contradiction:

Starting with $c_0 := a_j$ we would find some $c_1 := a'_j \in R$ such that $c_0 = d c_1$. As we can repeat the construction there is some $c_2 \in R$ such that $c_1 = d c_2$ which again is $c_0 = d^2 c_2$. Iterating we find $c_m \in R$ such that $c_0 = d^m c_m$ for any $m \in \mathbb{N}$. That is $d^m \mid a_j \neq 0$ for any $m \in \mathbb{N}$. But $d \notin R^*$ has a prime factor, so the fact that m can be increased indefinitely contradicts the primary decomposition of a_j which only admits finitely many prime divisors. The only way to avoid this contradiction is to have $a_j = 0$ which falsifies $q < r$.

(vii) As $M = F \oplus T$ and $\operatorname{rank}(F) = f$ and $\operatorname{rank}(T) = r$ according to (vi) it is clear that $\operatorname{rank}(M) = f + r$ by construction of the direct sum.

□

Proof of (5.32):

(iii) As M is finitely generated we have $N := \operatorname{rank}(M) \in \mathbb{N}$. And as $M \neq 0$ we also have $N \geq 1$. If $\{\, x_i \mid i \in 1 \ldots N \,\} \subseteq M$ is a generating set of M, then we have an epimorphism of the form

$$\psi \;:\; R^N \;\twoheadrightarrow\; M \;:\; (b_1, \ldots, b_N) \;\mapsto\; \sum_{i=1}^{N} b_i x_i$$

Let us take $P := \operatorname{kn}(\psi) \;\leq_{\mathfrak{m}}\; R^N$, then by the first isomorphism theorem of modules (3.78.(ii)) we find an induced isomorphism

$$\Psi \;:\; R^N \big/ P \;\xrightarrow{\sim}\; M \;:\; (b_1, \ldots, b_N) + P \;\mapsto\; \sum_{i=1}^{N} b_i x_i$$

But as R^N is a free R-module we may apply (5.28.(iv)) to find a basis $\{\, m_1, \ldots, m_N \,\}$ of R^N and subsets $\{\, p_1, \ldots, p_n \,\} \subseteq \{\, m_1, \ldots, m_N \,\}$ and $\{\, d_1, \ldots, d_n \,\} \subseteq R$ such that $\{\, d_i p_i \mid i \in 1 \ldots n \,\}$ is a

basis of P and $d_{i-1} \mid d_i$ for any $i \in 2 \dots n$. Without loss of generality we may assume $p_i = m_i$ for any $i \in 1 \dots n$.

Let us now define $M_i := Rm_i \ \leq_{\mathfrak{m}} \ R^N$ for any $i \in 1 \dots N$. Then R^N is the inner direct sum of the M_i, as the m_i form a basis of R^N. Also let $P_i := Rd_i m_i \ \leq_{\mathfrak{m}} \ M_i$ for any $i \in 1 \dots n$ and $P_j := 0 \ \leq_{\mathfrak{m}} \ M_j$ for $j \in (n+1) \dots N$. Then

$$\sum_{i=1}^{N} P_i \ = \ \mathsf{Lh}\{ d_1 m_1, \dots, d_n m_n \} \ = \ P$$

Thus by (3.35) we obtain another isomorphism of R-modules, this time

$$\Phi \ : \ \bigoplus_{i=1}^{N} M_i \Big/ P_i \ \xrightarrow{\sim} \ R^N \Big/ P \ : \ (y_i + P_i) \ :\mapsto \left(\sum_{i=1}^{N} y_i \right) + P$$

Let us denote $d_i := 0$ for $i \in (n+1) \dots N$ then [as any $m_i \neq 0$ and R is an integral domain, even a PID] it is clear, that for any $i \in 1 \dots N$ we have the isomorphy $R/d_i R \xrightarrow{\sim} M_i/P_i$ of R-modules given by $a_i + d_i R \mapsto a_i m_i + P_i$. Thus we can reformulate this isomorphy, as

$$\Phi' \ : \ \bigoplus_{i=1}^{N} R \Big/ d_i R \ \xrightarrow{\sim} \ R^N \Big/ P \ : \ (a_i + d_i R) \ :\mapsto \left(\sum_{i=1}^{N} a_i m_i \right) + P$$

Note that $\sum_i a_i m_i$ is some element $(b_1, \dots, b_N)$ of R^N. Thus we can compose $\Psi\Phi'$ to find the isomorphism we desired

$$\Psi\Phi' \ : \ \bigoplus_{i=1}^{N} R \Big/ d_i R \ \xrightarrow{\sim} \ M$$

All we need to do is analyze the structure of the module on the left-hand side. If $i > n$ then we have $d_i = 0$ and hence $R/d_i R \ \cong_{\mathfrak{m}} \ R$ canonically. However these are the only d_i with $d_i = 0$, since: If we had $d_1 = 0 \in R$ then we had $d_1 p_1 = 0 \in P$ such that $\{ d_1 p_1 \}$ would be linearly dependent. As $\{ d_i p_i \mid i \in 1 \dots n \}$ is a basis of P, this cannot be and hence we know $d_i \neq 0$ for any $i \in 1 \dots n$. Thus we may take $f := N - n$ and have

$$\Psi\Phi' \ : \ \bigoplus_{i=1}^{n} R \Big/ d_i R \oplus R^f \ \xrightarrow{\sim} \ M$$

And if $d_i \in R^*$ then $d_{i-1} \in R^*$ as well: By assumption $d_{i-1} \mid d_i$ we have $d_{i-1} a_i = d_i$ for some $a_i \in R$ and hence $d_{i-1}(a_i d_i^{-1}) = 1$ such that $d_{i-1} \in R^*$ as well. By induction we see there is a maximal number $z \in \mathbb{N}$ such that $d_i \in R^*$ for any $i \leq z$ that is

$$d_i \ \in \ \begin{cases} R^* \text{ if } i \in 1 \dots z \\ R^\bullet \text{ if } i \in (z+1) \dots n \end{cases}$$

However if $d_i \in R^*$ then $R/d_i R = 0$ so we might as well omit these direct summands. And if we

define $r := n - z$ then the above isomorphism may be rewritten once more, into

$$\Psi\Phi' \; : \; \bigoplus_{i=1}^{r} R \Big/ d_{z+i}R \oplus R^f \;\; \xrightarrow{\sim} \;\; M$$

Thus renumbering the $d_i := d_{z+i}$ we have found the invariant factors of M that have all the properties we asked for. Note that since R is a PID it also is an UFD by (2.79.(ii)) and hence the additional statements concerning M are just taken from (5.31). Note that $N = \mathrm{rank}(M) = r + f = n - z + N - n = N - z$, that is $z = 0$ which means that by minimality of the generating set $\{ x_1, \ldots, x_N \}$ there are *no* $d_i \in R^*$ in the first place.

(i) By (iii) we have an isomorphism of the form [for some $r, f \in \mathbb{N}$ with $n = \mathrm{rank}(M) = f + r$ according to (5.31.(vii)) and some invariant factors $d_i \in R$ such that $d_1 \mid d_2$ until $d_{n-1} \mid d_n$]

$$\Phi \; : \; \left(\bigoplus_{i=1}^{r} R \Big/ d_i R \right) \oplus R^f \;\; \xrightarrow{\sim} \;\; M$$

For ease of notation we let $d_i := 0$ for any $i \in (r+1) \ldots n$, such that R is isomorphic to $R/0 = R/d_iR$ and we can rewrite the isomorphism

$$\Phi \; : \; \bigoplus_{i=1}^{n} R \Big/ d_i R \;\; \xrightarrow{\sim} \;\; M$$

Let us then denote $g_1 := (1 + d_1R, 0 + d_2R, \ldots, 0 + d_nR)$ and so on, until $g_n := (0 + d_1R, \ldots, 0 + d_{n-1}R, 1 + d_nR)$. Then it is clear, that

$$R \;\; \twoheadrightarrow \;\; Rg_i \; : \; a \;\mapsto\; ag_i$$

has the kernel d_iR. But as this is the annihilator of g_i we find $\mathrm{ann}(g_i) = d_iR$. If we now let $m_i := \Phi(g_i) \in M$, then we will see, that

$$M \;\; = \;\; Rm_1 \oplus \cdots \oplus Rm_n$$

As the g_i generate M and Φ is surjective the m_i generate M. Conversely if $x \in Rm_j \cap \sum_{i \neq j} Rm_i$ then, as Φ also is injective, its preimage is contained in $\Phi^{-1}(x) \in Rg_j \cap \sum_{i \neq j} Rg_i = 0$, such that $x = 0$. But these are the two properties required for an inner direct sum.

As Φ is an isomorphism we have $\mathrm{ann}(m_i) = \mathrm{ann}(g_i) = d_iR$ and thereby the ascending chain of divisibilities $d_{i-1} \mid d_i$ turns into a descending chain of ideals $\mathrm{ann}(m_{i-1}) = d_{i-1}R \;\supseteq\; d_iR = \mathrm{ann}(m_i)$. In particular

$$\mathrm{ann}(M) \;\; = \;\; \bigcap_{i=1}^{n} \mathrm{ann}(m_i) \;\; = \;\; \mathrm{ann}(m_n)$$

Also for any $i \leq j \in 1 \ldots n$ we have $d_i \mid d_j$ and thereby $d_jm_i = 0$. For any $x = \sum_i a_im_i \in M$ this means $d_jx = \sum_i a_id_jm_i \in M$ where all summands with $i \leq j$ are deleted. Therefore we have $d_jM \subseteq Rm_{j+1} + \cdots + Rm_n$ such that we have

$$d_j \;\; \in \;\; \mathrm{ann}\left(M \Big/ Rm_{j+1} + \cdots + Rm_n \right)$$

And as the annihilator is an ideal it already contains d_jR. Conversely if $am_j + (Rm_{j+1} + \cdots + Rm_n) = 0$ then $am_j \in (Rm_j) \cap (Rm_{j+1} + \cdots + Rm_n) = 0$ such that $a \in \operatorname{ann}(m_j) = d_jR$. That is we also have

$$d_jR \;=\; \operatorname{ann}\left(M \Big/ Rm_{j+1} + \cdots + Rm_n\right)$$

(v) Let us first consider R/dR for some $d \in R$. As the PID R is a factorial ring, according to (2.79.(ii)), we find a primary decomposition

$$d \;=\; \alpha \prod_{j=1}^{s} p(j)^{m(j)}$$

of d, where $\alpha \in R^*$ and $m(j) \in \mathbb{N}$ and the $p(j) \in R$ are pairwise non-associated primes of R. In particular: If we abbreviate $a_j := p(j)^{m(j)}$ and pick up some prime $q \in R$, then $q \mid a_j$ and $q \mid a_k$ would imply $q \mid p(j)$ and $q \mid p(k)$ such that $p(j) \approx q \approx p(k)$, which is untrue. Therefore we have $1 \in \gcd\{\, a_j, a_k \,\}$ and as R is a PID we find that the ideals $\mathfrak{a}_j := a_jR$ and $\mathfrak{a}_k = a_kR$ are coprime $\mathfrak{a}_j + \mathfrak{a}_k = R$, according to the lemma of Bezout (2.83.(iii)).

But the intersection of all these ideals is dR: By definition $b \in \mathfrak{a}_j = a_jR$ is equivalent to $a_j \mid b$ such that $d \in \mathfrak{a}_j$ for any $j \in 1 \ldots s$. This is $dR \subseteq \bigcap_j \mathfrak{a}_j$. Conversely if $p(j)^{m(j)} = a_j \mid b$, then $m(j) \leq \langle p(j) \mid b \rangle$ and if this is true for any $j \in 1 \ldots s$, then $d \mid b$, such that $\bigcap_j \mathfrak{a}_j \subseteq dR$, as well. Now the Chinese remainder theorem (1.99.(iii)) yields the isomorphism

$$R \Big/ dR \;\xrightarrow{\sim}\; \bigoplus_{j=1}^{s} R \Big/ p(j)^{m(j)}R \;:\; b + dR \mapsto \left(b + p(j)^{m(j)}R\right)$$

After these preparations, let us turn to the claim at hand: If we pick up a primary decomposition of $d_r = \alpha_r\, p(1)^{m(1)} \ldots p(j)^{m(j)}$, then by assumption we have $d_i \mid d_r$ for any $i \in 1 \ldots r$. And by (2.64.(iii)) this means $\langle p(j) \mid d_i \rangle \leq \langle p(s) \mid d_i \rangle = m(j)$ which means, that we find a primary decomposition of any d_i in terms of the same prime factors

$$d_i \;=\; \alpha_i \prod_{j=1}^{s} p(j)^{m(i,j)}$$

where $m(i,j) = \langle p(j) \mid d_i \rangle$ (where we allow $m(i,j) = 0$ here). It is clear then for any $j \in 1 \ldots s$ the powers $m(1,j) \leq \cdots \leq m(r,j)$ form ascending chains. And as we have seen above, we have the isomorphies

$$R \Big/ d_iR \;\xrightarrow{\sim}\; \bigoplus_{j=1}^{s} R \Big/ p(j)^{m(i,j)}R \;:\; b + d_iR \mapsto \left(b + p(j)^{m(i,j)}R\right)$$

All we have to do is rearrange the summands in the exterior direct sum (obviously transposing the direct sum preserves the isomorphy)

$$\bigoplus_{i=1}^{r} R \Big/ d_iR \;\cong_{\mathfrak{m}}\; \bigoplus_{i=1}^{r}\bigoplus_{j=1}^{s} R \Big/ p(j)^{m(i,j)}R \;=\; \bigoplus_{j=1}^{s}\bigoplus_{i=1}^{r} R \Big/ p(j)^{m(i,j)}R$$

This almost is the representation of the claim: All we have to do is reverse the order of $m(1,j) \leq \cdots \leq m(r,j)$, by taking to the powers $n(i,j) := m(r+1-i,j)$ for $i \in 1 \ldots r$ and $j \in 1 \ldots s$. That

is the $n(i,j)$ are the same powers, but now $n(1,j) \geq \cdots \geq n(r,j)$. Note that there may still be some $n(i,j) = 0$, but in this case $p(j)^{n(i,j)} = 1$ such that $R/p(j)^{n(i,j)}R = 0$. Hence we can omit the direct summands with $n(i,j) = 0$ and define $I(j) := \max\{\, i \in 1 \ldots r \mid n(i,j) \neq 0 \,\}$. Then we arrive at the isomorphy of

$$\bigoplus_{i=1}^{r} R \Big/ d_i R \;\cong_{\mathfrak{m}}\; \bigoplus_{j=1}^{s} \bigoplus_{i=1}^{r} R \Big/ p(j)^{m(i,j)} R \;=\; \bigoplus_{j=1}^{s} \bigoplus_{i=1}^{I(j)} R \Big/ p(j)^{n(i,j)} R$$

And clearly this isomorphism can be extended by the free module R^f, such that we finally have the desired isomorphy of

$$\bigoplus_{i=1}^{r} R \Big/ d_i R \oplus R^f \;\cong_{\mathfrak{m}}\; \bigoplus_{j=1}^{s} \bigoplus_{i=1}^{I(j)} R \Big/ p(j)^{n(i,j)} R \oplus R^f$$

(iv) Consider the following R modules, where the elements $d_1, \ldots, d_r \in R$ and $e_1, \ldots, e_s \in R$ are invariant factors of a common module

$$\begin{aligned} M &:= R^f \oplus \bigoplus_{i=1}^{r} R \Big/ d_i R \\ N &:= R^g \oplus \bigoplus_{j=1}^{s} R \Big/ e_j R \end{aligned}$$

By assumption we have $M \cong_{\mathfrak{m}} N$, the base ring R is a PID and hence an UFD so that according to (5.31) this is $f = \mathrm{free}(M) = \mathrm{free}(N) = g$ and $f + r = \mathrm{rank}(M) = \mathrm{rank}(N) = g + s$. Since $f = g$ the latter implies $r = s$. But according to (3.23.(v)) we then have $\mathrm{TOR}(M) \cong_{\mathfrak{m}} \mathrm{TOR}(N)$ which now is

$$\bigoplus_{i=1}^{r} R \Big/ d_i R \;\cong_{\mathfrak{m}}\; \bigoplus_{i=1}^{r} R \Big/ e_i R$$

This isomorphy implies $e_r \in \mathrm{ann}(\mathrm{TOR}(M)) = d_r R$ and conversely $d_r \in e_r R$ such that $e_r = u_r d_r$ for some unit $u_r \in R^*$. Recall that we denote this by writing $d_r \approx e_r$. We now use induction on the length $\ell(e_i)$ of the primary decomposition of e_i, that is on the number of prime divisors of e_i (counting multiplicities).

If we start with any prime $p \in R$ and let $F := R/pR$ then F is a field, since $pR \trianglelefteq_{\mathfrak{i}} R$ is a maximal ideal of R. Also by (3.46) we have

$$M_p \;\cong_{\mathfrak{m}}\; \bigoplus_{i=1}^{r} \left(R \Big/ e_i R \right)_p \;\cong_{\mathfrak{m}}\; \bigoplus_{i=1}^{r} \begin{cases} F \text{ if } p \mid e_i \\ 0 \text{ if } p \not| e_i \end{cases}$$

Note that (3.46) also tells us, that M_p is an F-vector-space and by definition $(a + pR)m = am$ any R-linear map automatically is F-linear, too. Hence the above isomorphism of R-modules also is an isomorphism of F-vector-spaces, such that we find

$$\dim\left(M_p\right) \;=\; \#\{\, i \in 1 \ldots r \mid p \mid e_i \,\}$$

In complete analogy $\dim(M_p) = \#\{\, i \in 1\ldots r \mid p \mid e_i \,\}$. So if we start with a prime divisor of e_1 we get from $e_1 \mid e_2$ and so on until $e_{r-1} \mid e_r$ that $p \mid e_i$ for any $i \in 1\ldots r$. That is we conclude $r = \dim(M_p)$ for any prime divisor of e_1. In turn this implies $p \mid d_1$. Reversing the argument we find that e_1 and d_1 have the same prime factors (but they do not necessarily share the same multiplicities), yet we do not requires this observation for the rest of our proof.

We are now ready to present the foundation of our induction: Suppose $\ell(e_1) = 1$, i.e. $p := e_1$ is a prime itself. As $e_1 \notin R^*$ and $e_1 \mid e_2$ and so on until $e_{r-1} \mid e_r = p$ we find $e_i \approx p$ for any $i \in 1\ldots r$. As we have already argued $d_r \approx e_r = p$ such that in complete analogy we have $d_i \approx p$ for any $i \in 1\ldots r$. And in particular this implies $d_i \approx e_i$ for any $i \in 1\ldots r$.

For the induction step we start with any prime factor p of e_1, that is $p \mid e_1$ which is possible, since neither $e_1 \in R^*$ nor $e_i = 0$. Then we have $p \mid e_1 \mid e_i$ and hence $p \mid e_i$ for any $i \in 1\ldots r$ again. Let us write $e_i = p\varepsilon_i$ for some $\varepsilon_i \in R$. Now (3.46.(v)) constructs a new isomorphy

$$\textsc{tor}(M) \;\cong_{\mathsf{m}}\; \bigoplus_{i=1}^{r} R\Big/_{e_i R} \quad\Longrightarrow\quad p\,\textsc{tor}(M) \;\cong_{\mathsf{m}}\; \bigoplus_{i=1}^{r} R\Big/_{\varepsilon_i R}$$

As we have seen above, $p \mid e_1$ also implies $p \mid d_1$ and as $d_1 \mid d_2$ and so on until $d_{r-1} \mid d_r$ this is $p \mid d_i$ for any $i \in 1\ldots r$. So let us write $d_i = p\delta_i$ for some $\delta_i \in R$. Repeating the argument of (3.46.(v)) yields

$$\bigoplus_{i=1}^{r} R\Big/_{\delta_i R} \;\cong_{\mathsf{m}}\; p\,\textsc{tor}(M) \;\cong_{\mathsf{m}}\; \bigoplus_{i=1}^{r} R\Big/_{\varepsilon_i R}$$

Note that $\ell(e_r) = \ell(e_r) - 1 < \ell(e_r)$ such that the induction hypothesis implies $\varepsilon_i = u_i\delta_i$ for some $u_i \in R^*$ for any $i \in 1\ldots r$. Multiplying this by p we arrive at $e_i = u_i d_i$ which had to be shown. Thus we conclude the induction step and hence the proof.

(ii) Since M is the (inner) direct sum of the sub-modules Rp_i the p_i generate M and hence there is an epimorphism ϱ of the form

$$\varrho \;:\; R^m \twoheadrightarrow M \;:\; (a_i) \mapsto \sum_{i=1}^{m} a_i p_i$$

As R is a PID we may pick up some $d_i \in R$ such that for any $i \in 1\ldots m$ we have $\operatorname{ann}(p_i) = d_i R$. It is clear, that $d_i \notin R^*$ as we would else have $\operatorname{ann}(p_i) = R$ and hence p_i would not not occur at all and hence the sum of the Rp_i would not have been direct. Let $r := \max\{\, i \in 0\ldots m \mid d_i \neq 0 \,\}$, then we have $d_i \in R^\bullet$ for any $i \in 1\ldots r$ and $d_i = 0$ for $i \in (r+1)\ldots m$. As we have $d_i R = \operatorname{ann}(p_i) \subseteq \operatorname{ann}(p_{i-1}) = d_{i-1}R$ we also see $d_{i-1} \mid d_i$. So the d_i satisfy all the properties required for elementary divisors. We now claim that the kernel of ϱ is given to be

$$\operatorname{kn}(\varrho) \;=\; d_1R \oplus \cdots \oplus d_rR \oplus 0 \oplus \cdots \oplus 0$$

Clearly if $a = (a_i) \in R^m$ such that $a_i \in d_iR$ for any $i \in 1\ldots m$, then $a_i p_i = 0$ and hence $\varrho(a) = 0$. Conversely if $\varrho(a) = 0$ then $a_i p_i = 0$ for any $i \in 1\ldots m$, as the sum of the Rp_i has been direct. But this again means $a_i \in \operatorname{ann}(p_i) = d_i R$. Now the first isomorphism theorem of modules applied

to ϱ induces an isomorphism of the form

$$\bigoplus_{i=1}^{r} R\Big/_{d_iR} \oplus R^f \;=\; \bigoplus_{i=1}^{m} R\Big/_{d_iR} \;:\xrightarrow{\sim}\; M \;:\; \Big(a_i + d_iR\Big) \mapsto \sum_{i=1}^{m} a_i p_i$$

where $f := m - r$. The same arguments can be applied to the direct sum of M factored into Rq_j where $j \in 1 \dots n$. That is we obtain another isomorphy of the form

$$\bigoplus_{j=1}^{s} R\Big/_{e_jR} \oplus R^g \;:\xrightarrow{\sim}\; M \;:\; \Big(b_j + e_jR\Big) \mapsto \sum_{j=1}^{n} b_j q_j$$

where $e_jR = \operatorname{ann}(q_j)$ and $s := \max\big\{\, j \in 0 \dots n \mid e_j \neq 0 \,\big\}$ and $g := n - s$. In particular the direct sums of the R/d_iR and R/e_jR are isomorphic and hence we may invoke (iv) to find $r = s$ and $f = g$ and some $u_i \in R^*$ such that $e_i = u_i d_i$ for any $i \in 1 \dots r$. But this means $\operatorname{ann}(p_i) = d_iR = e_iR = \operatorname{ann}(q_i)$ for any $i \in 1 \dots r$ already. Also $m = r + f = s + g = n$ and for any $j \in (r+1) \dots n$ we have $\operatorname{ann}(p_j) = 0 = \operatorname{ann}(q_j)$. Altogether the uniqueness has been established.

(vi) Reversing the construction in (v) we let $r := \max\{\, I(j) \mid j \in 1 \dots s \,\}$ and $n(i,j) := 0$ for $I(j) < i \leq r$ and finally for any $i \in 1 \dots r$

$$d_i \;:=\; \prod_{j=1}^{s} p(j)^{n(r+1-i,j)}$$

That is we reconstruct the invariant factors from the elementary divisors. Then we have $d_i \neq 0$ (as R is an integral domain) and $d_i \notin R^*$ as at least one $n(r,j) \geq 1$ is non-zero. As $n(r,j) \leq \dots \leq n(1,j)$ we find that $d_1 \mid d_2$ and so on, until $d_{r-1} \mid d_r$. The arguments of (v) apply again, so we end up with the following isomorphy

$$\bigoplus_{i=1}^{r} R\Big/_{d_iR} \oplus R^f \quad\cong_{\mathsf{m}}\quad \bigoplus_{j=1}^{s} \bigoplus_{i=1}^{I(j)} R\Big/_{p(j)^{n(i,j)}R} \oplus R^f \quad\cong_{\mathsf{m}}\quad M$$

Likewise we take $q := \max\{\, K(\ell) \mid \ell \in 1 \dots t \,\}$ and define e_k to be the product of the $q(\ell)^{m(q+1-k,\ell}$ where ℓ rund from 1 to t. Then we get the second isomorphy

$$\bigoplus_{k=1}^{q} R\Big/_{e_kR} \oplus R^g \quad\cong_{\mathsf{m}}\quad M$$

As both are isomorphic to M we can invoke (iv) to see that $r = q$, $f = g$ and $e_i = u_i d_i$ for some $u_i \in R^*$ for any $i \in 1 \dots r$. Explicitly that is (for any $i \in 1 \dots r$)

$$\prod_{\ell=1}^{t} q(\ell)^{m(r+1-i,\ell)} \;=\; u_i \prod_{j=1}^{s} p(j)^{n(r+1-i,j)}$$

That is we have found two prime decompositions of e_i, but these are essentially unique, that is we may apply (2.58.(viii)). Applying this to $i = r$ this theorem tells us that any $p(j)$ is the associate of some $q(\ell)$. As the $p(j)$ (likewise the $q(\ell)$ are pairwise non-associated the s distinct primes $q(j)$ correspond to the $t = s$ distinct primes $q(\ell)$. I.e. there is a permutation σ of $1 \dots s$ such that $p(j) \approx q(\sigma(j))$. And if $q(j)$ appears $n(r+1-i,j)$-times in d_i then $q(\sigma(j))$ appears just as often

in e_i (this includes the cases where d_i does not appear at all, i.e. when $n(r+1-i,j)=0$). That is we have $m(r+1-i,\sigma(j))=n(r+1-i,j)$ for any $i \in 1\dots r$ and any $j \in 1\dots s$. Reversing the order by going to $h=r+1-i$ we have $m(h,\sigma(j))=n(h,j)$ for any $h \in 1\dots r$, as claimed. And as the minimum $h \in 1\dots r$ such that $n(h,j)=0$ is the same for $m(h,\sigma(j))$ we see $I(j)=K(\sigma(j))$. That is all the uniqueness properties of the claim are satisfied.

□

15.7 Proofs of Chapter 6

Proof of (6.3):
First of all, it is clear that $\sim$ truly is an equivalence relation: As $d(x,x) = 0$ we have the reflexivity $x \sim x$. And if $x \sim y$ then $d(y,x) = d(x,y) = 0$ by (M3), such that $y \sim x$ again, this is the symmetry of the relation. And if $x \sim y$ and $y \sim z$, then by (M1) and (M4) we have

$$0 \;\leq\; d(x,z) \;\leq\; d(x,y) + d(y,z) \;=\; 0 + 0 \;=\; 0$$

such that we get $x \sim z$ from $d(x,z) = 0$, which is the transitivity of the relation. Let us prove the well-definedness of $D([x],[y]) := d(x,y)$ next: That is we consider any $u \in [x]$ and $v \in [y]$ and need to show $d(u,v) = d(x,y)$. By assumption $u \in [u]$ we have $u \sim x$ such that $d(u,x) = 0$, likewise $v \sim y$, such that $d(v,y) = 0$. Then we get

$$d(u,v) \;\leq\; d(u,x) + d(x,v) \;=\; d(x,v) \;\leq\; d(x,y) + d(y,v) \;=\; d(x,y)$$

That is $d(u,v) \leq d(x,y)$ and in complete analogy we find $d(x,y) \leq d(u,v)$. Hence $d(u,v) = d(x,y)$ are equal and thereby D is well-defined. It remains to prove that D is a metric: (M1) $D([x],[y]) = d(x,y) \geq 0$ and (M3) $D([x],[y]) = d(x,y) = d(y,x) = D([y],[x])$ are obvious. The triangle inequality of D is also inherited from d, as $D([x],[z]) = d(x,z) \leq d(x,y) + d(y,z) = D([x],[y]) + D([y],[z])$. So for (M2) finally: If $D([x],[y]) = 0$, then $d(x,y) = 0$ such that $x \sim y$, which means $[x] = [y]$, altogether D is a metric. □

Proof of (6.4):

(i) Let $\delta := d(x,y)$, as $y \in B_r(x)$ we have $\delta < r$ by definition of the open balls. Now let $\varepsilon := (r-\delta)/2$, then we have $0 < \varepsilon \leq r/2 < r$ again. We now claim that $B_\varepsilon(y) \subseteq B_r(x)$. That is we consider any $z \in B_\varepsilon(y)$, which means $d(y,z) < \varepsilon$. Then we compute

$$d(x,z) \;\leq\; d(x,y) + d(y,z) \;<\; \delta + \varepsilon \;=\; \delta + \frac{r-\delta}{2} \;=\; \frac{r+\delta}{2} \;>\; r$$

In particular $z \in B_r(x)$ and as this is true for any $z \in B_\varepsilon(y)$ we have $B_\varepsilon(y)$. In particular for $P = B_r(x)$ we get: If $y \in P$, then $B_\varepsilon(y) \subseteq P$, which makes P an open subset of X.

(ii) As $x \neq y$ we have $r := d(x,y) > 0$. Now let $\varepsilon := r/3$ and define $U := B_\varepsilon(x)$ and $V := B_\varepsilon(y)$. Then $x \in U$ and $y \in V$ are obvious. Also U and V are open subsets of X, by (i). It remains to prove $U \cap V = \emptyset$. Thus assume $z \in U \cap V$, then from $z \in U = B_\varepsilon(x)$ we would get $d(x,z) < \varepsilon$ and likewise $d(y,z) < \varepsilon$ from $z \in V = B_\varepsilon(y)$. But then we had $d(x,y) < r$, in contradiction, to $d(x,y) = r$, as we would be able to compute

$$d(x,y) \;\leq\; d(x,z) + d(z,y) \;<\; \varepsilon + \varepsilon \;=\; \frac{2}{3}r \;<\; r$$

(iii) The "open" part of property (1) has been proved in (i). And $x \in B_r(x)$ is true for any $r > 0$, as $d(x,x) = 0 < r$. Property (2) is obvious, as $y \in F_{n+1}(x)$ means $d(x,y) < 1/(n+1) < 1/n$ which implies $y \in F_n(x)$. For (3) we consider some $y \in X$ such that $y \in F_n(x)$ for any $n \in \mathbb{N}$. Let $r := d(x,y)$ then $y \in F_n(x)$ means $r < 1/n$. And as this is true for any $n \in \mathbb{N}$ this can

only be $r = 0$. But as d is a metric, this means $y = x$ again. Finally (4) is immediate from the definition of open sets: If $U \subseteq X$ is open and $x \in U$, then by definition we have $B_r(x) \subseteq U$ for some $r > 0$. Now simply take $n \in \mathbb{N}$ such that $1/n \leq r$, then $F_n(x) = B_{1/n}(x) \subseteq B_r(x) \subseteq U$. Property (5) is a slight refinement of (ii): Given $x \neq y \in X$ let $r := d(x,y)$ and choose $n \in \mathbb{N}$ such that $1/n \leq \varepsilon := r/3$. Then we get $F_n(x) \subseteq B_\varepsilon(x)$ and $F_n(y) \subseteq B_\varepsilon(y)$. And thereby $F_n(x) \cap F_n(y) \subseteq B_\varepsilon(x) \cap B_\varepsilon(y) = \emptyset$, as we have seen in (ii). In particular $F_n(x) \cap F_n(y) = \emptyset$.

In property (6) we have $F_0(x) = X$ for any $x \in X$, by definition. So we only have to deal with the second part of (6): That is we consider some $F, G \in \mathcal{F}$, say $F = F_m(y)$ and $G = F_n(z)$ and an element $x \in F \cap G$. Recall that $F = B_{1/m}(y)$ and $G = B_{1/n}(z)$ and let $\varepsilon(y) := (1/m - d(x,y))/2$ and $\varepsilon(z) := (1/n - d(x,z))/2$. Note that $\varepsilon(y)$ and $\varepsilon(z) > 0$, as $x \in F$ and $x \in G$ respectively. Also may choose some $k \in \mathbb{N}$ such that $1/k \leq \min\{\, \varepsilon(y), \varepsilon(z) \,\}$, then by (i) we have $B_{1/k}(x) \subseteq B_{\varepsilon(y)}(x) \subseteq B_{1/m}(y) = F$ and analogously $B_{1/k}(x) \subseteq B_{\varepsilon(z)}(x) \subseteq B_{1/n}(z) = G$. Thus if we take $E := B_{1/k}(x)$, then we have $x \in E = F_k(x)$ and $E \subseteq F \cap G$, as required.

□

Proof of (6.6):

- We start with (a) $\implies$ (b): That is we are given $x \in X$ and $\varepsilon > 0$ and need to find a sufficient $\delta > 0$. Abbreviate $V := B_\varepsilon(Y, f(x))$, which is an open set in Y. By assumption (a) we know that $U := f^{-1}(V) = \{\, y \in X \mid f(y) \in V \,\}$ is an open set of X. Also $x \in U$, as $f(x) \in V$. By the definition of open sets, this means $B_\delta(X,x) \subseteq U$ for some $\delta > 0$. Thus for any $y \in B_\delta(X,x)$ we have $y \in U = f^{-1}(V)$ such that $f(y) \in V = B_\varepsilon(Y, f(x))$, which is (b) precisely.

- Conversely, for (b) $\implies$ (a): We begin with an open set $V \subseteq Y$ and let $U := f^{-1}(V)$. We need to show, that $U \subseteq X$ is open, that is for any $x \in U$ there has to be some $r > 0$ such that $B_r(x) \subseteq U$. As $x \in U$ we have $f(x) \in V$ and as $V \subseteq Y$ is open, this means $B_\varepsilon(Y, f(x)) \subseteq V$ for some $\varepsilon > 0$. Choose $\delta > 0$ such that $y \in B_\delta(X,x)$ implies $f(y) \in B_\varepsilon(Y, f(x)) \subseteq V$. Then $f(y) \in V$ means $y \in f^{-1}(V) = U$. And as this is true for any $y \in B_\delta(X,x)$ we have $B_\delta(X,x) \subseteq U$. Thus (by taking $r := \delta$) we proved, that $U = f^{-1}(V)$ is an open subset of X, again.

- Now to (b) $\implies$ (c): That is we are given a converging sequence $(x_n) \to x$ and need to show $(f(x_n)) \to f(x)$. The latter is: Given any $\varepsilon > 0$ there is some $n(\varepsilon) \in \mathbb{N}$ such that for any $n \geq n(\varepsilon)$ we have $f(x_n) \in B_\varepsilon(Y, f(x))$. By assumption (b) there is some $\delta > 0$ such that for any $y \in B_\delta(X,x)$ we have $f(y) \in B_\varepsilon(Y, f(x))$. Also $(x_n) \to x$, which means, that there is some $n(\delta) \in \mathbb{N}$ such that for any $n \geq n(\delta)$ we have $x_n \in B_\delta(X,x)$. Thus for $y = x_n$ for some $n \geq n(\delta)$ we get $x_n \in B_\delta(X,x)$ and hence $f(x_n) \in B_\varepsilon(Y, f(x))$. So by taking $n(\varepsilon) := n(\delta)$ we are done.

- It remains to verify (c) $\implies$ (b): Here we start with some $x \in X$ and $\varepsilon > 0$ again and need to find a sufficient $\delta > 0$. Assume this was false - there is no such δ. This means that for any $\delta > 0$ there is some $y \in B_\delta(X,x)$ such that $f(y) \notin B_\varepsilon(Y, f(x))$. For any $n \in \mathbb{N}$ take $\delta := 1/(n+1)$ then there is some $x_n \in B_\delta(X,x)$ such that $f(x_n) \notin B_\varepsilon(Y, f(x))$. Let us verify, that for this sequence we have $(x_n) \to x$: Given $r > 0$ take $n(r) \in \mathbb{N}$ in such a way, that $1/n(r) \leq r$. Then for any $n \geq n(r)$ we get $1/n \leq 1/n(r) \leq r$. For x_n we have $d(x, x_n) < 1/(n+1) < 1/n \leq \varepsilon$, by construction. Thus $x_n \in B_r(X,x)$ for any $n \geq n(r)$, which is the definition of $(x_n) \to x$. Thus by assumption (c) we have $(f(x_n)) \to f(x)$, too. Yet by construction we have $f(x_n) \notin B_\varepsilon(Y, f(x))$ for any $n \in \mathbb{N}$. In

particular $f(x_n) \to f(x)$ is impossible. This contradiction can only be solved, if there was some $\delta > 0$ with the desired property, to begin with.

□

Proof of (6.8):

(i) Consider any $y \in B_{r/M}(D,x)$, that is $D(x,y) < r/M$. By assumption we have the following estimate: $d(x,y) \leq M \cdot D(x,y) < r$ and thereby $y \in B_r(d,x)$. As this is true for any y we have the inclusion $B_{r/M}(D,x) \subseteq B_r(d,x)$.

(ii) As $d \leq D$ there is some $M > 0$ such that the assumption in (i) is always satisfied. Now consider any $U \subseteq \mathcal{T}_d$, that is for any $x \in U$ there is some $r > 0$ such that $B_r(d,x) \subseteq U$. But then we have seen in (i), that $B_{r/M}(D,x) \subseteq B_r(d,x) \subseteq U$. As $r/M > 0$, still this means that $U \in \mathcal{T}_D$ and as this is true for any U we have the inclusion $\mathcal{T}_d \subseteq \mathcal{T}_D$.

(iii) We have to prove $(x_n) \to_d x$ which means that for any $\varepsilon > 0$ there has to be some $n(\varepsilon) \in \mathbb{N}$, such that for any $n \geq n(\varepsilon)$ we find $x_n \in B_\varepsilon(d,x)$. But as $(x_n) \to_D x$ and $\varepsilon/M > 0$, still there is some $n(\varepsilon) \in \mathbb{N}$ such that for any $n \geq n(\varepsilon)$ we have $x_n \in B_{\varepsilon/M}(D,x)$. Now by (i) we have $B_{\varepsilon/M}(D,x) \subseteq B_\varepsilon(d,x)$, such that $x_n \in B_\varepsilon(d,x)$ is true. Thus we have found $(x_n) \to_d x$, as well.

□

Proof of (6.16):

(i) Let us denote $\mathcal{U}(P) := \{\, U \subseteq X \text{ open} \mid U \subseteq P \,\}$, then P° has been defined, as the grand union $P^\circ = \bigcup \mathcal{U}(P)$. Note that $\emptyset$ is open and hence $\emptyset \in \mathcal{U}(P)$. But by definition of a topology any union of open sets is open, in particular $P^\circ = \bigcup \mathcal{U}(P)$ is open. It remains to verify

$$P^\circ \;=\; \{\, x \in P \mid \exists\, U \subseteq X \text{ open} : x \in U \subseteq P \,\}$$

If $x \in P$ admits some U with $x \in U \subseteq P$, then $U \in \mathcal{U}(P)$ and hence $U \subseteq P^\circ$ such that $x \in P^\circ$. Conversely if $x \in P^\circ$, then there is some $U \in \mathcal{U}(P)$ with $x \in U$. But then $x \in U \subseteq P$ makes x an element of the right-hand set.

(ii) Let us denote $\mathcal{Z}(P) := \{\, C \subseteq X \text{ closed} \mid P \subseteq C \,\}$, then $\overline{P}$ has been defined, as the intersection $\overline{P} = \bigcap \mathcal{Z}(P)$. Note that X is closed and hence $X \in \mathcal{Z}(P)$, such that the intersection is well-defined (it runs over a non-empty set). By (6.10) any non-empty intersection of closed sets is closed again, in particular $\overline{P} = \bigcap \mathcal{Z}(P)$ is closed. It remains to verify $\overline{P} = X \setminus Q^\circ$ for $Q := X \setminus P$. But this is a simple consequence of complements: Let $C := X \setminus U$, which is a closed set of X, then

$$\begin{aligned}
X \setminus Q^\circ &= X \setminus \bigcup \{\, U \mid U \subseteq X \text{ open}, U \subseteq Q \,\} \\
&= \bigcap \{\, X \setminus U \mid U \subseteq X \text{ open}, U \subseteq Q \,\} \\
&= \bigcap \{\, C \mid C \subseteq X \text{ closed}, X \setminus C \subseteq Q \,\} \\
&= \bigcap \{\, C \mid C \subseteq X \text{ closed}, C \supseteq X \setminus Q \,\} \\
&= \bigcap \{\, C \mid C \subseteq X \text{ closed}, C \supseteq P \,\} \;=\; \overline{P}
\end{aligned}$$

(iii) Just note that $\partial P = \overline{P} \setminus P^\circ$ can also be written, as $\partial P = \overline{\mathcal{P}} \cap (X \setminus P^\circ)$ and this is an intersection of closed sets, by (ii) and (i) respectively, and thereby this is a closed set again.

(vi) By construction any $U \in \mathcal{U}(P)$ is contained in $U \subseteq P$. Thus if we consider any $x \in P^\circ = \bigcup \mathcal{U}(P)$, then $x \in U$ for some $U \in \mathcal{U}(P)$ and as $U \subseteq P$ this yields $x \in P$. Therefore we have $P^\circ \subseteq P$. Likewise for any $C \in \mathcal{Z}(P)$ we have $P \subseteq C$. So if we start with any $x \in P$, then $x \in C$ for any $C \in \mathcal{Z}(P)$. But this means $x \in \bigcap \mathcal{Z}(P) = \overline{P}$, such that we get the inclusion $P \subseteq \overline{P}$, as well.

(iv) By (i) U° is open, thus if $U = U^\circ$ then U already is open. Conversely, if U is open, then $U \in \mathcal{U}(U)$ and therefore $U \subseteq \bigcup \mathcal{U}(U) = U^\circ$. But $U^\circ \subseteq U$ is generally true, by (vi) and therefore $U = U^\circ$.

(v) By (ii) $\overline{C}$ is closed, thus if $C = \overline{C}$, then C already is closed. Conversely, if C is closed, then $C \in \mathcal{Z}(C)$ and therefore $\overline{C} = \bigcap \mathcal{Z}(C) \subseteq C$. But $C \subseteq \overline{C}$ is generally true and therefore $C = \overline{C}$.

(vii) By definition we have $\partial P = \overline{P} \setminus P^\circ$. Taking the union with P° on both sides, we alredy get the claim $\partial P \cup P^\circ = (\overline{P} \setminus P^\circ) \cup P^\circ = \overline{P}$ already.

(viii) Let us denote $\mathcal{Z}(P) := \{ Z \subseteq X \text{ closed} \mid P \subseteq Z \}$, then $C \in \mathcal{Z}(P)$ by assumption. And by definition we have $\overline{P} = \bigcap \mathcal{Z}(P)$, but $\bigcap \mathcal{Z}(P) \subseteq C$, as C is part of this grand intersection.

(ix) By (i) we have $V^\circ = \{ x \in V \mid \exists U \in \mathcal{T}(x) : U \subseteq V \}$. And by assumption we have $x \in V^\circ$ for any $x \in V$. This is $V \subseteq V^\circ$ and as $V^\circ \subseteq V$ is generally true by (vi), we get $V = V^\circ$. But by (iv) this means that V is open.

(x) By definition the closure of P in S is the intersection of all closed subsets in S that contain P. And by construction of the relative topology a subset $C \subseteq S$ is closed, iff it is of the form $C = D \cap S$ for some closed subset $D \subseteq X$. Therefore we have

$$\mathrm{cl}_S(P) \;=\; \bigcap \{ C \subseteq S \text{ closed} \mid P \subseteq C \} \;=\; \bigcap \{ D \cap S \mid D \subseteq X \text{ closed}, P \subseteq D \cap S \}$$

As $P \subseteq S$ is given $P \subseteq D \cap S$ is equivalent to $P \subseteq D$. Also we can pull out $\cap S$ from the grand intersection, as it always is the same set. But doing this we see, that the expression left is just the closure of P as a subset of X and thereby

$$\overline{P} \;=\; \bigcap \{ D \mid D \subseteq X \text{ closed}, P \subseteq D \} \cap S \;=\; \mathrm{cl}_X(P) \cap S$$

□

Proof of (6.12):

(i) Clearly $\emptyset = \emptyset \cap S$ and as $S \subseteq X$ also $S = X \cap S$, such that properties (T1) and (T2) are satisfied for $\mathcal{T} \cap S$. Also if $U \cap S$ and $V \cap S \in \mathcal{T} \cap S$, then $(U \cap S) \cap (V \cap S) = (U \cap V) \cap S$ and as $U \cap V \in \mathcal{T}$ again this is property (T3). Likewise for any $\{ U_i \cap S \mid i \in I \}$ where $U_i \in \mathcal{T}$ for any $i \in I$ it is clear that $\bigcup_i (U_i \cap S) = (\bigcup_i U_i) \cap S$ and by assumption we have $\bigcup_i U_i \in \mathcal{T}$ again. That is $\bigcup_i (U_i \cap S) \in \mathcal{T} \cap S$ and this has been property (T4) of the topology $\mathcal{T} \cap S$.

(ii) (T1) is due to (C2): $\emptyset = X \setminus X \in \mathcal{T}$ and (T2) is due to (C1): $X = X \setminus \emptyset \in \mathcal{T}$. (T3) is due to (C3) by going to complements: If $U = X \setminus C$ and $V = X \setminus D$ then $U \cap V = (X \setminus C) \cap (X \setminus D) = X \setminus (C \cup D)$

where we have $C \cup D \in \mathcal{Z}$, such that $U \cap V \in \mathcal{T}$ again. Likewise (T4) is due to (C4) by going to complements: Consider any $\mathcal{U} = \{ U_i \mid i \in I \}$ where $U_i = X \setminus C_i$ for some $C_i \in \mathcal{Z}$, by assumption. Then $\bigcup_i U_i = \bigcup (X \setminus C_i) = X \setminus (\bigcap_i C_i)$ and as $\bigcap_i C_i \in \mathcal{Z}$ again, this implies $\bigcup_i U_i \in \mathcal{T}$.

(iii) Let us prove prove that $\mathcal{T} := \{ U \subseteq X \mid \text{(a)} \}$ is a topology on X: Property (T1) is trivial: As $\emptyset$ does not contain any elements, there is nothing to prove. (T2) is "X is an open set": But by (B1) any $x \in X = \bigcup \mathcal{B}$ is contained in some $B \in \mathcal{B}$. And $B \subseteq X$ is trivial, such that we have $x \in B \subseteq X$, as required. Now for (T3) we are given two open sets $U, V \in X$ and need to show, that $U \cap V$ is open again. Hence we consider any $x \in U \cap V$: As $x \in U$ there is some $B \in \mathcal{B}$ with $x \in B \subseteq U$, likewise there is some $C \in \mathcal{B}$ with $x \in C \subseteq V$. In particular $x \in B \cap C$. Now by (B2) there is some $A \subseteq \mathcal{B}$ such that $x \in A \subseteq B \cap C$. As $B \subseteq U$ and $C \subseteq V$ we have $B \cap B \subseteq U \cap V$ and thereby $x \in A \subseteq U \cap V$, as required for an open set. Finally for (T4) we are given a collection $\mathcal{U} = \{ U_i \mid i \in I \}$ of open sets in X and need to prove that it satisfies (a) again: Consider some $x \in \bigcup_i U_i$. That is $x \in U_j$ for some $j \in I$. And as U_j is open this means that there is some $B \in \mathcal{B}$ such that $x \in B \subseteq U_j$. In particular $U_j \subseteq \bigcup_i U_i$ and hence $x \in B \subseteq \bigcup_i U_i$.

(iii) In the second step, let us verify, that for any subset $U \subseteq X$ the properties (a) and (b) are equivalent: We begin with (b) $\implies$ (a): Given any $x \in U = \bigcup_i B_i$ there is some $j \in I$ with $x \in B_j$. On the other hand we have $B_j \subseteq \bigcup_i B_i = U$ such that $x \in B_j \subseteq U$ for some $B_j \in \mathcal{B}$. Conversely (a) $\implies$ (b): That is for any $x \in U$ there is some base set $B_x \in \mathcal{B}$ with $x \in B_x$ and $B_x \subseteq \mathcal{B}$. Let us take $I := U$, then we claim that $\{ B_x \mid x \in U \}$ satisfies $U = \bigcup_x B_x$. For any $x \in U$ we have $x \in B_x$ such that $U \subseteq \bigcup_x B_x$. Conversely if $y \in \bigcup_x B_x$ then there is some $x \in U$ such that $y \in B_x$. But as $B_x \subseteq U$ this yields $y \in U$ such that $\bigcup_x B_x \subseteq U$, as well.

(iv) Recall that for any $U \subseteq X$ we have $U \in \mathcal{T}$ if and only if $U \in \mathcal{T}_i$ for any $i \in I$. (T1) As $\emptyset \in \mathcal{T}_i$ for any $i \in I$ we have $\emptyset \in \mathcal{T}$ again. (T2) The same $X \in \mathcal{T}$ is true, as $X \in \mathcal{T}_i$ for any $i \in I$, too. (T3) Consider $U, V \in \mathcal{T}$, that is $U, V \in \mathcal{T}_i$ for any $i \in I$. As $\mathcal{T}_i$ is a topology we have $U \cap V \in \mathcal{T}_i$ again. And as this is true for any $i \in I$, we conclude $U \cap V \in \mathcal{T}$. (T4) We are given some $\mathcal{U} \subseteq \mathcal{T}$, that is any $U \in \mathcal{U}$ is contained in $U \in \mathcal{T}$ and thereby $U \in \mathcal{T}_i$ for any $i \in I$. As this is true for any $U \in \mathcal{U}$ we have $\mathcal{U} \subseteq \mathcal{T}_i$ again. Now $\mathcal{T}_i$ is a topology and hence $\bigcup \mathcal{U} \in \mathcal{T}_i$. And as this is true for any $i \in I$ we conclude $\bigcup \mathcal{U} \in \mathcal{T}$.

(v) (T1) is clear, as $\emptyset = f^{-1}(\emptyset)$ and likewise (T2) is satisfied, because of $X = f^{-1}(Y)$. (T3) consider $U_1, U_2 \in f^{-1}(\mathcal{T}_Y)$, that is $U_i = f^{-1}(V_i)$ for some $V_i \subseteq Y$ open. Then by (0.7) we have $f^{-1}(V_1 \cap V_2) = f^{-1}(V_1) \cap f^{-1}(V_2) = U_1 \cap U_2$ and as $V_1 \cap V_2 \in \mathcal{T}_Y$ this means $U_1 \cap U_2 \in f^{-1}(\mathcal{T}_Y)$ again. (T4) consider $\mathcal{U} = \{ U_i \mid i \in I \} \subseteq f^{-1}(\mathcal{T}_Y)$ that is any $U_i \in \mathcal{U}$ is of the form $U_i = f^{-1}(V_i)$ for some $V_i \in \mathcal{T}_Y$. Then by (0.7) we also have $f^{-1}(\bigcup_i V_i) = \bigcup_i f^{-1}(V_i) = \bigcup_i U_i$ and as $\bigcup_i V_i \in \mathcal{T}_Y$ this means $\bigcup_i U_i \in f^{-1}(\mathcal{T}_Y)$, as well.

(vi) Let us abbreviate the cartesian product by $X := \prod_i X_i$ and the following subset $\mathcal{B}$ of $\mathcal{P}(X)$. We will prove that $\mathcal{B}$ is the basis of a topology on X, where

$$\mathcal{B} \;:=\; \left\{ \prod_{i \in I} U_i \;\middle|\; \forall\, i \in I \,:\, U_i \subseteq X_i \text{ open} \right\}$$

Property (B1) is clear, as we even have $X = \prod_i X_i \in \mathcal{B}$. Now consider $B = \prod_i U_i$ and $C =$

$\prod_i V_i \in \mathcal{B}$, such that $(x_i) \in B \cap C$. That is $x_i \in U_i \cap V_i$ and $U_i \cap V_i \in \mathcal{T}_i$ again. Thus we can define $A := \prod_i (U_i \cap V_i) \in \mathcal{B}$ and thereby have $(x_i) \in A$ and $A \subseteq B \cap C$. That is $\mathcal{B}$ satisfies (B1) and (B2) in (iii) and thereby $\prod_i \mathcal{T}_i$ is a topology on X.

□

Proof of (6.18):

(i) Let $C \subseteq \bigcup_i U_i$ (where $i \in I$) be an open cover of C. As C is closed, $V := X \setminus C$ is open and hence we find an open cover of X, by adding V to the cover of C:

$$X \;=\; C \cup (X \setminus C) \;=\; \bigcup_{i \in I} U_i \cup V$$

As X is compact there is a finite subset $\Omega \subseteq I$ such that $X = \bigcup_i U_i \cap V$ where i runs in $i \in \Omega$. But as $V \cap V = \emptyset$, intersecting this identity with C we find, that these U_i already cover C

$$C \;=\; X \cap C \;=\; \bigcup_{i \in \Omega} U_i \cap C \;\subseteq\; \bigcup_{i \in \Omega} U_i$$

(ii) Let $K := K_1 \cup \cdots \cup K_n$ be the union of these sets and consider an open cover $K \subseteq \bigcup_i U_i$ (where i runs in some set $i \in I$). For any $j \in 1 \ldots n$ we have $K_j \subseteq K \subseteq \bigcup_i U_i$ such that the compactness of K_j yields a finite subset $\Omega(j) \subseteq I$ such that $K_j \subseteq \bigcup_i U_i$ where this i runs in $i \in \Omega(j)$. Now let $\Omega := \Omega(1) \cup \cdots \cup \Omega(n) \subseteq I$, which again is a finite set. Then we find a finite subcover of K, by

$$K \;=\; \bigcup_{j=1}^{n} K_j \;\subseteq\; \bigcup_{j=1}^{n} \bigcup_{i \in \Omega(j)} U_i \;=\; \bigcup_{i \in \Omega} U_i$$

□

Proof of (6.21):

(i) The implication (a) $\Longrightarrow$ (b) is trivial: This is property (F3) of a system of local filters. Conversely for (b) $\Longrightarrow$ (a) we start with an arbitrary subset $U \subseteq X$ satisfying (b). That is for any $x \in U$ there is some index $n \in \mathbb{N}$ such that $F_n(x) \subseteq U$. Thereby we may take $n(x) \in \mathbb{N}$ to be the minimal index, such that $U_x := F_{n(x)}(x) \subseteq U$. By (F1) $U_x \subseteq X$ is an open subset, with $x \in U_x$ and. And as $U_x \subseteq U$ by construction, it is clear that

$$U \;=\; \bigcap_{x \in U} U_x$$

That is: U is the union of a collection of open subsets $U_x \subseteq X$. And by property (T4) of a topology, this union is open again. And as the union equals U, this means $U \subseteq X$ is open.

(ii) If $\mathcal{F}$ is a system of local filters, then $(X, \mathcal{T})$ is a Hausdorff-space: Consider any two $x \neq y$ then by (F4) there is some $n \in \mathbb{N}$, such that $F_n(x) \cap F_n(y) = \emptyset$. But by (F1) $F_n(x) \in \mathcal{T}(x)$ and $F_n(y) \in \mathcal{T}(y)$ these are open sets, containing x and y respectively. Also $\mathcal{F}$ already is a countable filter base of $(X, \mathcal{T})$: By assumption (F1) we have $F_n(x) \in \mathcal{T}(x)$ and $\mathcal{F}(x) = \{\, F_n(x) \mid n \in \mathbb{N} \,\}$ is

countable by construction. Also, we have already shown that any $U \in \mathcal{T}(x)$ contains some $F_n(x)$ in the implication (a) $\implies$ (b) of (i).

Conversely suppose (1) and (2), then we have to construct a system of local filters of X: By assumption $\mathcal{B}(x)$ is countable, so let us do this $\mathcal{B}(x) = \{ B_n(x) \mid n \in \mathbb{N} \}$ in any order, whatsoever. Then we define

$$F_n(x) \;:=\; \bigcap_{k=0}^{n} B_k(x)$$

As $\mathcal{B}(x) \subseteq \mathcal{T}(x)$ we have $x \in F_n(x)$ again. And as $F_n(x)$ is a *finite* intersection of open sets, it is open, too. That is for any $n \in \mathbb{N}$ we have $F_n(x) \in \mathcal{T}(x)$ again, which is (F1). The $F_n(x)$ form a descending chain by construction, so (F2) is satisfied, as well. Now, if $U \in \mathcal{T}(x)$, then there is some $B \in \mathcal{B}(x)$, such that $B \subseteq U$. Say $B = B_n(x)$, then $F_n(x) \subseteq B_n(x) = B \subseteq U$, which is property (F3). Finally for (F4): Given $x \neq y \in X$ there are some open sets $U, V \subseteq X$, such that $x \in U$, $y \in V$ and $U \cap V = \emptyset$, due to (1). That is $U \in \mathcal{T}(x)$ and $V \in \mathcal{T}(y)$. As we just argued, there is some $r \in \mathbb{N}$, such that $F_r(x) \subseteq U$ and likewise $F_s(y) \subseteq V$ for some $s \in \mathbb{N}$. Now let $n := \max\{ r, s \}$, then $F_n(x) \subseteq F_r(x) \subseteq U$ and $F_n(y) \subseteq F_s(y) \subseteq V$. In particular $F_n(x) \cap F_n(y) \subseteq U \cap V = \emptyset$, such that $F_n(x) \cap F_n(y) = \emptyset$.

(iii) (1) If $(x_n) \subseteq X$ is a sequence for which there is some $N \in \mathbb{N}$, such that for any $n \geq N$ we have $x_n = x$, then for any $m \in \mathbb{N}$ we can take $n(m) := m$, as for this we get $x_n = x \in F_m(x)$ for any $n \geq N = n(m)$. (2) Suppose $(x_n) \to_{\mathcal{F}} x$ and $(x_n) \to_{\mathcal{F}} y$ for some $x, y \in X$. That is for any $m \in \mathbb{N}$ there were some $r(m), s(m) \in \mathbb{N}$ such that $x_n \in F_m(x)$ for any $n \geq r(m)$ respectively $x_n \in F_m(y)$ for any $n \geq s(m)$. Let $n(m) := \max\{ r(m), s(m) \}$, then for any $n \geq n(m)$ we had $x_n \in F_m(x) \cap F_m(y)$. That is for any $m \in \mathbb{N}$ we have $F_m(x) \cap F_m(y) \neq \emptyset$ and by property (F4) this can only happen, in case $x = y$.

(iv) By the symmetry of the situation it suffices to prove one implication of the equivalence. So let us assume $(x_n) \to_{\mathcal{F}} x$ and we would like to show $(x_n) \to_{\mathcal{E}} x$. That is for any $m \in \mathbb{N}$ we need to find some $n(m) \in \mathbb{N}$ such that for any $n \geq n(m)$ we get $x_n \in E_m(x)$. But $E_m(x) \in \mathcal{T}(x)$ such that by (F3) of $\mathcal{F}$ there is some $r(m) \in \mathbb{N}$ such that $F_{r(m)}(x) \subseteq E_m(x)$. Also we have $(x_n) \to_{\mathcal{F}} x$ such that there is some $s(r(m)) \in \mathbb{N}$ such that for any $n \geq s(r(m))$ we have $x_n \in F_{r(m)}(x)$. Now let $n(m) := s(r(m))$, then for any $n \geq n(m)$ we have $x_n \in F_{r(m)}(x) \subseteq E_m(x)$. And thereby we have established $(x_n) \to_{\mathcal{E}} x$.

(v) For the inclusion from right to left we start with a sequence $(x_n) \subseteq P$ that converges $(x_n) \to_{\mathcal{F}} x$ for some $x \in X$ and need to show $x \in \overline{P}$. Suppose this was false, i.e. $x \notin \overline{P}$. That is $x \in U := X \setminus \overline{P}$, which is an open set in X. By (6.16.(vi)) we have $P \subseteq \overline{P}$ and therefore $U = X \setminus \overline{P} \subseteq Q := X \setminus P$. By (6.15) we even have $\overline{P} = X \setminus Q^\circ$ which is $U = Q^\circ$. We have assumed $x \in U$, that is $x \in Q^\circ$ and need to find a contradiction. Thus take a look at the interior of Q, by (6.15) again, this is

$$Q^\circ \;=\; \{ x \in Q \mid \exists\, V \subseteq X \text{ open} : x \in V \subseteq Q \}$$

As $x \in Q^\circ$ there is some $V \subseteq X$ open, such that $x \in V$ and $V \subseteq Q = X \setminus P$. As $V \in \mathcal{T}(x)$ and $\mathcal{F}$ is a system of local filters there is some $m \in \mathbb{N}$, such that $F_m(x) \subseteq V$. Recall that we also have $(x_n) \to_{\mathcal{F}} x$, that is for any $m \in \mathbb{N}$ there is some $n(m) \in \mathbb{N}$ such that for any $n \geq n(m)$ we have

$x_n \in F_m(x)$. In particular $x_{n(m)} \in F_m(x) \subseteq V \subseteq Q = X \setminus P$. But this contradicts $(x_n) \subseteq P$, as this would imply $x_{n(m)} \in P$. Thus the assumption $x \notin \overline{P}$ cannot be and hence $x \in \overline{P}$.

(v) For the inclusion from left to right we start with some $x \in \overline{P}$ and need to find a sequence $(x_n) \subseteq P$ such that $(x_n) \to_{\mathcal{F}} x$. By (6.15) again, we have $\overline{P} = X \setminus Q^\circ$ where $Q := X \setminus P$. As $x \in \overline{P}$ we have $x \notin Q^\circ$ and this means:

$$\forall\, V \subseteq X \text{ open } :\ x \notin V \text{ or } V \not\subseteq Q$$

Thereby $V \not\subseteq Q$ means, there is some $y \in V$ with $y \notin Q$. And as $Q = X \setminus P$ this is $y \in P$. In other words there is some $y \in V$ with $y \in P$ and thereby $y \in V \cap P$, such that $V \cap P \neq \emptyset$. So let us rewrite the above statement with this in mind

$$\forall\, V \subseteq X \text{ open } :\ x \notin V \text{ or } V \cap P \neq \emptyset$$

In particular we can use this property for $V = F_n(x)$, as this is an open set in X. That is for any $n \in \mathbb{N}$ we have $x \notin F_n(x)$ or $F_n(x) \cap P \neq \emptyset$. As $F_n(x) \in \mathcal{T}(x)$ we have $x \in F_n(x)$ such that there has to be some $x_n \in F_n(x) \cap P$. As this is true for any $n \in \mathbb{N}$ we have found a sequence $(x_n) \subseteq P$. It only remains to prove $(x_n) \to_{\mathcal{F}} x$. That is we need to check that for all $m \in \mathbb{N}$ there has to be some $n(m) \in \mathbb{N}$, such that for any $n \geq n(m)$ we have $x_n \in F_m(x)$. But by construction we can take $n(m) := m$, then $x_n \in F_n(x) \subseteq F_m(x)$ for any $n \geq m$, such that $(x_n) \to_{\mathcal{F}} x$.

(vi) For the implication (a) $\implies$ (b) we start with a closed set $C \subseteq X$ and consider a convergent sequence $(x_n) \to_{\mathcal{F}} x$. Then by (v) we have $x \in \overline{C}$, but as C is closed this is $x \in C$, as$C = \overline{C}$, due to (6.16.(v)).

Conversely for (b) $\implies$ (a) we consider any $x \in \overline{C}$. By (v) this means $(x_n) \to x$ for some sequence $(x_n) \subseteq C$. But by assumption (b) this means $x \in C$ again and as this is true for any $x \in \overline{C}$, we have established $\overline{C} \subseteq C$. But $C \subseteq \overline{C}$ is generally true, by (6.16.(vi)) and hence $C = \overline{C}$. But by (6.16.(v)) this means that C is closed.

□

Proof of (6.23):

(i) As X is an open subset of X and $x \in X$ we have $X \in \mathcal{T}(x)$ and hence $X \in \mathcal{N}(x)$. In particular $\mathcal{N}(x) \neq \emptyset$. Also if $N \in \mathcal{N}(x)$ then there is some $U \in \mathcal{T}(x)$ with $U \subseteq N$. But as $x \in U$, by definition of $\mathcal{T}(x)$, this yields $x \in N$ and hence $N \neq \emptyset$. The upward closure property is obvious: If $N \in \mathcal{N}(x)$ and $N \subseteq P$, then there is some $U \in \mathcal{T}(x)$ with $U \subseteq N \subseteq P$ and hence $P \in \mathcal{N}(x)$, again. Finally let M, $N \in \mathcal{N}(x)$, then there are some U, $V \in \mathcal{T}(x)$, such that $U \subseteq M$ and $V \subseteq N$. As $U \cap V$ and $x \in U \cap V$, too, we have $U \cap V \subseteq \mathcal{T}(x)$. Also $U \cap V \subseteq M \cap N$ such that $M \cap N \subseteq \mathcal{N}(x)$ again, which means that $\mathcal{N}(x)$ is also colsed under finite intersections.

(ii) As $\mathcal{F} \neq \emptyset$, there is some $F \in \mathcal{F}$ and therefore $f(F) \in f(\mathcal{F})$, such that $f(\mathcal{F}) \neq \emptyset$, as well. Also for any $F \in \mathcal{F}$ there is some $x \in F$. Thereby $f(x) \in f(F)$, such that $f(F) \neq \emptyset$, again. Now to the upward closure property of $f(\mathcal{F})$: Consider any $F \in \mathcal{F}$ and any $Q \subseteq Y$ such that $f(F) \subseteq Q$. Then we have to prove $Q \in f(\mathcal{F})$ again. Let $P := f^{-1}(Q)$, if we start with $x \in F$, then $f(x) \in f(F) \subseteq Q$ such that $x \in f^{-1}(Q) = P$. That is we have $F \subseteq P$ and as $\mathcal{F}$ is a prefilter,

this means $P \in \mathcal{F}$, as well. Now recall (0.7), where we proved that

$$f(P) \;=\; f\big(f^{-1}(Q)\big) \;=\; f(X) \cap Q$$

As f is surjective, this means $f(P) = Q$ and as $P \in \mathcal{F}$ we have found $Q \in f(\mathcal{F})$ again. Now let $\mathcal{F}$ be a filter, then $X \in \mathcal{F}$ and thereby $Y = f(X) \in f(\mathcal{F})$, as well. Also consider any two F, $G \in \mathcal{F}$, then we need to show $f(F) \cap f(G) \in f(\mathcal{F})$ again. Let $E := F \cap G$ which is an element of $E \in \mathcal{F}$ again, as $\mathcal{F}$ is a filter. Then $f(E) \subseteq f(F) \cap f(G)$ is generally true. But as $f(E) \in f(\mathcal{F})$ the upward closure property guarantees $f(F) \cap f(G) \in f(\mathcal{F})$, again.

(iii) First of all, there is some $B \in \mathcal{B}$ and as $B \subseteq X$ we find $X \in \mathcal{F}$. Now consider any F with $B \subseteq F$ for some $B \in \mathcal{B}$. As any $B \in \mathcal{B}$ satisfies $x \in B$ we have $x \in B \subseteq F$ and thereby $x \in F$, such that $F \neq \emptyset$. The upward closure property is clear again: Given any $P \subseteq X$ with $F \subseteq P$ we have $B \subseteq F \subseteq P$, such that $P \in \mathcal{F}$ again. Now for finite intersections: Consider another $G \in \mathcal{F}$ such that $C \subseteq E$, for some $C \in \mathcal{B}$. Then by assumption there is some $A \in \mathcal{B}$, such that $A \subseteq B \cap C$ and thereby $A \subseteq B \cap C \subseteq F \cap G$, such that $F \cap B \in \mathcal{F}$ again.

(iii) If there is some $n \in \mathbb{N}$ such that $F_n(x) \subseteq N$, then we readily have $N \in \mathcal{N}(x)$, as $F_n(x) \in \mathcal{T}(x)$ by property (F1) of a system of local filters. Conversely if $N \in \mathcal{N}(x)$, then there is some $U \in \mathcal{T}(x)$ with $U \subseteq N$. And by property (F3) there is some $n \in \mathbb{N}$ such that $F_n(x) \subseteq U \subseteq N$. Thus N is contained in the set generated by $\mathcal{F}(x)$.

□

Proof of (6.24):

- For (a) $\implies$ (b) we start with some closed set $D \subseteq Y$, that is $D = Y \setminus V$ for some open set $V \subseteq Y$. By (0.7) we have $f^{-1}(Y \setminus V) = X \setminus f^{-1}(V)$ such that $f^{-1}(D) = X \setminus f^{-1}(V)$. But by (a) $f^{-1}(V) \subseteq X$ is open and hence $f^{-1}(D) = X \setminus f^{-1}(V) \subseteq X$ is closed. The converse direction (b) $\implies$ (a) recycles this idea: If $V \subseteq Y$ is open, then $D := Y \setminus V$ is closed, so $f^{-1}(D)$ is closed. That is $U := X \setminus f^{-1}(D)$ is open. But $f^{-1}(V) = f^{-1}(Y \setminus D) = X \setminus f^{-1}(D) = U$ and hence $f^{-1}(V)$ is an open set in X.

- For (a) $\implies$ (c) we note, that $Q^\circ \subseteq Y$ is open. Therefore $f^{-1}(Q^\circ) \subseteq X$ is open, too. Generally $Q^\circ \subseteq Q$ such that $f^{-1}(Q^\circ) \subseteq f^{-1}(Q)$. That is $f^{-1}(Q^\circ)$ is an open set contained in $f^{-1}(Q)$. As $f^{-1}(Q)^\circ$ is the union of all such sets, we conclude $f^{-1}(Q^\circ) \subseteq f^{-1}(Q)^\circ$.

 Conversely for (c) $\implies$ (a) we start with some open set $V \subseteq Y$. As V is open, we have $V = V^\circ$ and thereby by assumption (c) also $f^{-1}(V) = f^{-1}(V^\circ) \subseteq f^{-1}(V)^\circ \subseteq f^{-1}(V)$. Thus we have $f^{-1}(V) = f^{-1}(V)^\circ$, which means that $f^{-1}(V)$ is an open subset of X.

- Let us prove (b) $\implies$ (d), that is we start with an arbitrary subset $Q \subseteq Y$. As $\overline{Q}$ is closed, (b) tells us $f^{-1}(\overline{Q}) \subseteq X$ is closed, too. Also $Q \subseteq \overline{Q}$ is generally true such that $f^{-1}(Q) \subseteq f^{-1}(\overline{Q})$. That is $f^{-1}(\overline{Q})$ is a closed set containing $f^{-1}(Q)$. As $\overline{f^{-1}(Q)}$ is the intersection of all such sets, we conclude $\overline{f^{-1}(Q)} \subseteq f^{-1}(\overline{Q})$.

 Conversely for (d) $\implies$ (b), we start with some closed set $D \subseteq Y$. As D is closed, we have $D = \overline{D}$ and thereby by assumption (d) also $f^{-1}(D) \subseteq \overline{f^{-1}(D)} \subseteq f^{-1}(\overline{D}) = f^{-1}(D)$. Thus we have $f^{-1}(D) = \overline{f^{-1}(D)}$, which means that $f^{-1}(D)$ is a closed subset of X.

- Let us prove (a) $\implies$ (f), that is we start with some $x \in X$ and $V \in \mathcal{T}(f(x))$ and need to find $U \in \mathcal{T}(x)$ such that $f(U) \subseteq V$. As $V \subseteq Y$ is open, so is $U := f^{-1}(V)$. And as $f(x) \in V$ we also have $x \in U = \{\, x \in X \mid f(x) \in V \,\}$. As we also have $f(U) = f\big(f^{-1}(V)\big) \subseteq V$ by (0.7) we have found the open neighbourhood U of x required.

 Conversely we prove (f) $\implies$ (c): That is we start with any subset $Q \subseteq V$ and need to prove $f^{-1}(Q^\circ) \subseteq f^{-1}(Q)^\circ$. Recall that these sets are given to be

$$\begin{aligned} Q^\circ &= \{\, y \in Q \mid \exists\, V \in \mathcal{T}(y) : V \subseteq Q \,\} \\ f^{-1}(Q)^\circ &= \Big\{\, x \in f^{-1}(Q) \mid \exists\, U \in \mathcal{T}(x) : U \subseteq f^{-1}(Q) \,\Big\} \end{aligned}$$

 So consider any $x \in f^{-1}(Q^\circ)$, that is $y := f(x) \in Q^\circ$ which means that there is some $V \in \mathcal{T}(y)$ such that $V \subseteq Q$. Note that $Q^\circ \subseteq Q$ also implies $y = f(x) \in Q$ and hence $x \in f^{-1}(Q)$. As $y = f(x)$ we have $V \in \mathcal{T}(f(x))$ and hence our assumption (f) yields some $U \in \mathcal{T}(x)$ such that $f(U) \subseteq V$. Yet by (0.7) $f(U) \subseteq V$ is equivalent to $U \subseteq f^{-1}(V)$. And as $V \subseteq Q$ we have $f^{-1}(V) \subseteq f^{-1}(Q)$. Let us summarize: We have found some $U \in \mathcal{T}(x)$ with $U \subseteq f^{-1}(Q)$ and $x \in f^{-1}(Q)$. This means $x \in f^{-1}(Q)^\circ$ and as this is true for any $x \in f^{-1}(Q^\circ)$ we have proved the inclusion required for (c).

- Now to (b) $\implies$ (e), that is we start with an arbitrary subset $P \subseteq X$. As $\overline{f(P)} \subseteq Y$ is closed, our assumption (b) implies, that $f^{-1}(\overline{f(P)}) \subseteq X$ is closed, too. Note that we generally have $P \subseteq f^{-1}(f(P))$ by (0.7) and also $f(P) \subseteq \overline{f(P)}$ by (6.16.(vi)). Therefore $P \subseteq f^{-1}(f(P)) \subseteq f^{-1}(\overline{f(P)})$. And as the latter set is closed in X we find $\overline{P} \subseteq f^{-1}(\overline{f(P)})$. By (0.7) again, this equivalent to $f(\overline{P}) \subseteq \overline{f(P)}$, which if property (e), as required.

 Conversely we want to prove (e) $\implies$ (f), that is we start with any $x \in X$ and $V \in \mathcal{T}(f(x))$ and need to find some $U \in \mathcal{T}(x)$ with $f(U) \subseteq V$. This can be done in the following way: Let $C := X \setminus f^{-1}(V) = f^{-1}(Y \setminus V)$. We know $Y \setminus V \subseteq Y$ is closed, but we don't know (yet), that $C \subseteq X$ is closed, too. As $C \subseteq f^{-1}(Y \setminus V)$ (they even are equal) we get $f(C) \subseteq Y \setminus V$ by (0.7) once more. But as $Y \setminus V$ is closed this means $\overline{f(C)} \subseteq Y \setminus V$. By assumption (e) we have $f(\overline{C}) \subseteq \overline{f(C)} \subseteq Y \setminus V$. Now let $U := X \setminus \overline{C}$ which is an open set of X, as $\overline{C}$ is guaranteed to be closed. As $f(x) \in V$ and $f(\overline{C}) \subseteq Y \setminus V$ we have $x \notin \overline{C}$ which means $x \in U$. Thus $U \in \mathcal{T}(x)$ is an open neighbourhood of x. As $C \subseteq \overline{C}$ we have $U = X \setminus \overline{C} \subseteq X \setminus C = f^{-1}(V)$ by construction of C. But $U \subseteq f^{-1}(V)$ again is equivalent to $f(U) \subseteq V$, which is just what we needed.

- Let us first prove (g) $\implies$ (f): To do this we choose $\mathcal{F} = \mathcal{N}(x)$ and we begin with some open neighbourhood $V \in \mathcal{T}(f(x))$. In particular $N := V \cap f(X) \in \mathcal{N}(f(x)) \subseteq f(\mathcal{F})$. That is there is some $M \in \mathcal{N}(x)$ such that $f(M) = N$. Now $M \in \mathcal{N}(x)$ means there is some $U \in \mathcal{T}(x)$ with $U \subseteq M$ and thereby $f(U) \subseteq f(M) = N = V \cap f(X) \subseteq V$.

 In the converse direction (f) $\implies$ (g) we are given some prefilter $\mathcal{F}$ such that $\mathcal{N}(x) \subseteq \mathcal{F}$ and some $N \in \mathcal{N}(f(x))$ and need to show $N \in f(\mathcal{F})$. By definition $N \in \mathcal{N}(f(x))$ means that there is some $V \in \mathcal{T}(f(x))$ such that $V \cap f(x) \subseteq N$. By assumption (f) there is some $U \in \mathcal{T}(x)$ such that $f(U) \subseteq V$ and as $f(U) \subseteq f(X)$ is clear, we have $f(U) \subseteq V \cap f(X) \subseteq N$. By assumption we have $U \in \mathcal{T}(x) \subseteq \mathcal{N}(x) \subseteq \mathcal{F}$ such that $f(U) \in f(\mathcal{F})$. Let us summarize: We have $f(U) \subseteq N \subseteq f(X)$ for some $f(U) \in f(\mathcal{F})$ and by (6.23.(ii)) $f(\mathcal{F})$ is a prefilter on $f(X)$.

Thus by the upward closure property this implies $N \in f(\mathcal{F})$. And as this is true for any N we have shown $\mathcal{N}(f(x)) \subseteq f(\mathcal{F})$, as claimed.

□

Proof of (6.25):

- Let us start with (a) $\implies$ (c), that is we have f continuous and $(x_n) \to_{\mathcal{E}} x$ and need to show $(f(x_n)) \to_{\mathcal{F}} f(x)$. That is we are given some $m \in \mathbb{N}$ and need to find some $n(m) \in \mathbb{N}$ such that for any $n \geq n(m)$ we have $f(x_n) \in F_m(f(x))$. Let us abbreviate $y := f(x)$, as $F_m(y) \subseteq Y$ is open and f is continuous the set $f^{-1}(F_m(y)) \subseteq X$ is open, too. And as $f(x) = y \in F_m(y)$ this set contains x. Therefore, by (6.21.(i)), there is some $r(m)$ such that $E_{r(m)}(x) \subseteq f^{-1}(F_m(y))$. And by (0.7) this is equivalent, to $f(E_{r(m)}(x)) \subseteq F_m(y)$. As $(x_n) \to_{\mathcal{E}} x$ there is some $n(m) \in \mathbb{N}$ such that for any $n \geq n(m)$ we get $x_n \in E_{r(m)}(x)$. And by construction this turns into $f(x_n) \in F_m(y) = F_m(f(x))$. And this is exactly what we need, for $(f(x_n)) \to_{\mathcal{F}} f(x)$.

- In the next step we are concerned with (c) $\implies$ (b), that is for any $n \in \mathbb{N}$ and any $x \in X$ we need to find some $m \in \mathbb{N}$, such that $f(E_m(x)) \subseteq F_n(f(x))$. Equivalently $E_m(x) \subseteq f^{-1}(F_n(y))$, where $y := f(x)$ again. Suppose this was *not* the case, that is for any $m \in \mathbb{N}$ the set $E_m(x)$ is *not* contained in $f^{-1}(F_n(y))$. That is for any $m \in \mathbb{N}$ there is some x_m such that $x_m \in E_m(x)$ but $x_m \notin f^{-1}(F_n(y))$. Then by construction we have $(x_m) \to_{\mathcal{E}} x$ because of: Take $n(m) := m$ then for any $n \geq n(m)$ we have $x_n \in E_n(x) \subseteq E_m(x)$. Thus by assumption (c) we also get $(f(x_n)) \to_{\mathcal{F}} f(x) = y$. This means, that there is some $r(n) \in \mathbb{N}$ such that for any $r \geq r(n)$ we get $f(x_r) \in F_n(y)$. In particular $x_{r(n)} \in f^{-1}(F_n(y))$ in contradiction to $x_m \notin f^{-1}(F_n(y))$ for any $m \in \mathbb{N}$. Thus no such sequence can exist and this means $E_m(x) \subseteq f^{-1}(F_n(y))$ for some $m \in \mathbb{N}$.

- To close the circle we need to prove (b) $\implies$ (a), that is we are given an open set $V \subseteq Y$ and need to prove that $U := f^{-1}(V) \subseteq X$ is open. To do this choose any $x \in U$ and let $y := f(x)$. As $x \in U = f^{-1}(V)$ we get $y = f(x) \in V$. And as V is open (6.21.(i)) tells us, that there is some $n \in \mathbb{N}$ such that $F_n(y) \subseteq V$. By assumption (b) this means, that there is some $m \in \mathbb{N}$, such that $f(E_m(x)) \subseteq F_n(y)$ and by (0.7) this is $E_m(x) \subseteq f^{-1}(F_n(y)) \subseteq f^{-1}(V) = U$. Thus for any $x \in U$ there is some $m \in \mathbb{N}$ such that $E_m(x) \subseteq U$, then by (6.21.(i)) again we conclude, that $U \subseteq X$ is open and hence f continuous.

□

Proof of (6.29):

(i) Let us denote $f_0 : x \mapsto y_0$, then for any subset $V \subseteq Y$ we have $f_0^{-1}(V) = X$ if $y_0 \in V$ and $f_0^{-1}(V) = \emptyset$ if $y_0 \notin V$. In both cases $f_0^{-1}(V) \in \mathcal{T}_X$ such that f_0 is continuous.

(ii) Clearly for any subset $U \subseteq X$ we have $\mathbb{1}_x^{-1}(U) = U$. Thus if $\mathbb{1}_X$ is continuous, then for any $U \in \mathcal{T}_2$ we have $U = \mathbb{1}_x^{-1}(U) \in \mathcal{T}_1$. And as this is true for any U we get $\mathcal{T}_2 \subseteq \mathcal{T}_1$. Conversely if $\mathcal{T}_2 \subseteq \mathcal{T}_1$, then $\mathbb{1}_x^{-1}(U) = U \in \mathcal{T}_1$ for any $U \in \mathcal{T}_2$, which means that $\mathbb{1}_X$ is continuous.

(iii) If we start with some open set $W \subseteq Z$, then $V := g^{-1}(W) \subseteq Y$ is open, as g is continuous. Now, as f is continuous, $U := f^{-1}(V) \subseteq X$ is open, too. But $(gf)^{-1}(W) = f^{-1}(g^{-1}(W)) = f^{-1}(V) = U \in \mathcal{T}_X$, which means that gf is continuous.

(iv) We have to show that $f^{-1}(V) \subseteq X$ is open, for any $V \subseteq Y$ open. As $\mathcal{B}$ is a base of the topology, there is some $\{ B_i \mid i \in I \} \subseteq \mathcal{B}$, such that $V = \bigcup_i B_i$. But then we get $f^{-1}(V) = \bigcup_i f^{-1}(B_i)$ by (0.7) and by assumption any $f^{-1}(B_i) \subseteq X$ is open. But then, by (T4), $f^{-1}(V)$ is open, as it is a union of open sets.

(v) We have to show that $f(U) \subseteq Y$ is open, for any $U \subseteq X$ open. As $\mathcal{A}$ is a base of the topology, there is some $\{ A_i \mid i \in I \} \subseteq \mathcal{A}$, such that $U = \bigcup_i A_i$. But then we get $f(U) = \bigcup_i f^(A_i)$ by (0.7) and by assumption any $f(A_i) \subseteq Y$ is open. But then, by (T4), $f(U)$ is open, as it is a union of open sets.

(vi) We have to show that $f(C) \subseteq Y$ is closed, for any $C \subseteq X$ closed. Being closed means $C = X \setminus U$ for some $U \subseteq X$ open. As $\mathcal{A}$ is a base of the topology, there is some $\{ A_i \mid i \in I \} \subseteq \mathcal{A}$, such that $U = \bigcup_i A_i$. But then $C = X \setminus \bigcup_i A_i = \bigcap_i X \setminus A_i$. As f is injective (0.7) tells us, that $f(C) = \bigcap_i f(X \setminus A_i)$ by (0.7). By assumption any $f(X \setminus A_i) \subseteq Y$ is closed and hence $f(C)$ is closed, as it is an intersection of closed sets.

(vii) If Φ is a homeomorphism, then φ is bijective and continuous by definition. Also $\Phi^{-1} : Y \to X$ is continuous. Now for any subset $P \subseteq X$ we find the identity

$$\left(\Phi^{-1}\right)^{-1}(P) \;=\; \left\{ y \in Y \mid \Phi^{-1}(y) \in P \right\} \;=\; \{ y \in Y \mid y \in \Phi(P) \} \;=\; \Phi(P)$$

Thus if $U \subseteq X$ is open, then $\Phi(U) = (\Phi^{-1})^{-1}(P) \subseteq Y$ is open as Φ^{-1} is continuous. If conversely Φ is open, then $\Phi(U)$ is open, such that Φ^{-1} is continuous. Likewise of closed sets: Φ^{-1} is continuous iff $\Phi^{-1}(C) \subseteq Y$ is closed, for any closed set $C \subseteq X$. And due to this identity this is true iff $\Phi(C)$ is closed for any closed set $C \subseteq X$, which is Φ is closed.

(viii) We need to prove that $f(K) \subseteq Y$ is compact, whenever $K \subseteq X$ is compact. So we start with an arbitrary open covering $\{ V_i \mid i \in I \} \subseteq \mathcal{T}_Y$ of $f(K)$. As $V_i \subseteq Y$ is open, so is $U_i := f^{-1}(V_i) \subseteq X$. If we consider any $x \in K$ then $f(x) \in f(K) \subseteq \bigcup_i V_i$ that is $f(x) \in V_i$ for some $i \in I$ and this is $x \in f^{-1}(V_i) = U_i$. Thus we see $K \subseteq \bigcup_i U_i$ (where $i \in I$) and as K is compact there is some finite subset $\Omega \subseteq I$ such that $K \subseteq \bigcup_i U_i$ (where $i \in \Omega$). That is any $x \in K$ is contained in some $U_i = f^{-1}(V_i)$ for some $i \in \Omega$. This means $f(x) \in V_i$ and as this is true for any $y = f(x) \in f(K)$ we find $f(K) \subseteq \bigcup_i V_i$ (where $i \in \Omega$). That is we have find a finite sub-cover $\{ V_i \mid i \in \Omega \}$, which was required for $f(K)$ to be compact.

(ix) Let us first prove, that π_j is continuous. That is for any open set $U_j \subseteq X_j$ we have to show, that $\pi_j^{-1}(U_j)$ is open again. The more restrictive topology is the product topology, in this case. But as

$$\pi_j^{-1}(U_j) \;:=\; \prod_{i \in I} \begin{cases} U_j \text{ if } i = j \\ X_i \text{ if } i \neq j \end{cases}$$

we see, that π_j^{-1} even is a base set of the product topology and in particular, this is an open set in $\prod_i X_i$. Thus π_j is continuous. Let us now prove that π_j also is open. In this case the box topology is the more restrictive, as it contains more open set. So let us start with an open set $W \subseteq \prod_i X_i$ that is: For any $(x_i) \in W$ there is a family of open neighbourhoods $U_i \in \mathcal{T}_i(x_i)$ such

that $\prod_i U_i \subseteq W$. It is clear, that

$$\pi_j\left(\prod_{i\in I} U_i\right) \;=\; U_j$$

We need to show that $\pi_j(W) \subseteq X_j$ is open. If $W = \emptyset$, then $\pi_j(W) = \emptyset$, too, which is an open set in X_j. So we only need to consider $W \neq \emptyset$. To show that $\pi_j(W)$ is open, it suffices, that $\pi_j(W) \subseteq \pi_j(W)^\circ$. Thus we start with some $x_j \in \pi_j(W)$. As $W \neq \emptyset$ so is $\pi_i(W) \subseteq X_i$ for any $i \in I$. Hence, for any $i \neq j$, we may choose some $x_i \in \pi_i(W)$, and compose these x_i with x_j to a point $(x_i) \in W$. As W is open there is some (U_i) with $U_i \in \mathcal{T}_i(x_i)$ and $\prod_i U_i \subseteq W$. In particular

$$x_j \;\in\; U_j \;=\; \pi_j\left(\prod_{i\in I} U_i\right) \;\subseteq\; \pi_j(W)$$

This means $x_i \in \pi_j(W)^\circ$ and thereby $\pi_j(W) \subseteq \pi_j(W)^\circ$. As the converse inclusion is generally true, we have $\pi_j(W) = \pi_j(W)^\circ$, which means, that $\pi_j(W)$ is open.

(x) To prove that $\prod_i f_i$ is continuous we have to verify, that $f^{-1}(W) \subseteq X$ is open, for any open subset $W \subseteq \prod_i Y_i$. So let us take a closer look at the preimage of W:

$$\begin{aligned}
\left(\prod_{i\in I} f_i\right)^{-1}(W) &= \left\{\, x \in X \mid \left(f_i(x)\right) \in W \,\right\} \\
&= \left\{\, x \in X \mid \forall\, i \in I : f_i(x) \in \pi_i(W) \,\right\} \\
&= \left\{\, x \in X \mid \forall\, i \in I : x \in f_i^{-1}\left(\pi_i(W)\right) \,\right\} \\
&= \bigcap_{i\in I} f_i^{-1}\left(\pi_i(W)\right)
\end{aligned}$$

If I is finite, the argument is easy: As W is open and any π_i is an open map, by (iv) we see that $\pi_i(W)$ is open. Also f_i is continuous and hence $f_i^{-1}(\pi_i(W)) \subseteq X$ is open. But a *finite* intersection of open sets is open again and hence the preimage of W under $\prod_i f_i$ is an open subset of X. This means $\prod_i f_i$ is continuous.

In case I is infinite we need to take a closer look at the product topology (and $\prod_i f_i$ need not be continuous if $\prod_i X_i$ is bestowed with the box topology): As W is open any point $y = (y_i) \in W$ is contained in a base set $\prod_i U_i \subseteq W$. For any $y \in W$ let $B(y) = \prod_i U_i(y) \in \mathcal{B}$ be some base set of the product topology, such that $y \in B(y) \subseteq W$. Then we get

$$W \;=\; \bigcup_{y\in W} B(y) \;=\; \prod_{i\in I}\left(\bigcup_{y\in W} U_i(y)\right)$$

Let $S(B(y)) := \{\, i \in I \mid U_i(y) \neq X_i \,\}$ be the set of indices for which $U_i(y)$ is not the entire space X_j. By construction of the product topology $S(B(y))$ is finite for any $y \in Y$. Also if $U_i(z) = X_i$ for some $z \in W$, then the union $\bigcup_y U_i(y) = X_i$ is full, as well. Thus $S(W) = \bigcap_y S(B(y))$ is contained in any $S(B(y))$ and hence finite, too. For any $i \notin S(W)$ we have $\pi_i(W) = \bigcup_y U_i(y) = X_i$ and hence $f_i^{-1}(\pi_i(W)) = X$. Thus no $i \notin S(W)$ contributes to the intersection above, the intersection runs over a finite subset of I only. And for finite sets I we already gave an argument. Thus in the product topology the preimage of W under $\prod_i f_i$ is an open subset of X, even if I is infinite.

(xi) For any $i \in I$ with $i \neq j$ let us denote the constant function $f_i : X_j \to X_i : x_j \mapsto a_i$. Then f_i is continuous, by (i). And for $i = j$ pick up the identity $\mathbb{1}_j : X_j \to X_j : x_j \mapsto x_j$. As both copies of X_j carry the same topology $\mathcal{T}_j$, the identity is continuous, according to (ii). Then by (vii) we find, that ι_j is continuous, as it is the product of

$$\iota_j \;=\; \prod_{i\in I} \begin{cases} \mathbb{1}_j \text{ if } i = j \\ f_i \text{ if } i \neq j \end{cases}$$

□

Proof of (6.31):

(i) We first have to prove that the final topology truly is a topology on Y: Clearly $f_i^{-1}(Y) = X_i$ and $f_i^{-1}(\emptyset) = \emptyset \subseteq X_i$ for any $i \in I$ such that Y and $\emptyset \subseteq Y$ are open. If now V_1 and $V_2 \subseteq Y$ are open sets, then $U_k := f_i(V_k) \subseteq X_i$ are open for any $i \in I$ and $k \in \{1,2\}$. But thereby

$$f_i^{-1}(V_1 \cap V_2) \;=\; f_i^{-1}(V_1) \cap f_i^{-1}(V_2) \;=\; U_1 \cap U_2 \;\subseteq\; X_i \text{ open}$$

as $\mathcal{T}_i$ is closed under finite intersections. Thereby $V_1 \cap V_2 \subseteq Y$ is open again. In complete analogy, for any index set K and open sets $V_k \subseteq X_i$ (where $k \in K$ and $U_k := f_i(V_k) \subseteq X_i$ again) we get by (0.7)

$$f_i^{-1}\left(\bigcup_{k\in K} V_k\right) \;=\; \bigcup_{k\in K} f_i^{-1}(V_k) \;=\; \bigcup_{k\in K} U_k \;\subseteq\; X_i \text{ open}$$

as $\mathcal{T}_i$ is closed under arbitrary unions. Again this means, that the union of the V_k is open in Y again. Altogether we have verified that we truly have a topology on Y. The fact that any f_i is continuous is just the construction of this topology: Consider any $i \in I$ and any open set $V \subseteq Y$. We have to show that $f_i^{-1}(V) \subseteq X_i$ is open. But this has just been the definition of "open" in Y.

(i) Now to the second part of (i), the equivalence of (a) and (b) for any map $g : Y \to Z$: If (a), then by (6.29.(iii)) the map $gf_i : X_i \to Z$ is continuous, too. Conversely, if (b) then we have to check that $g^{-1}(W) \subseteq Y$ is open, for any open subset $W \subseteq Z$. By definition $g^{-1}(W)$ is open iff for any $i \in I$ the set $f_i^{-1}(g^{-1}(W)) \subseteq X_i$ is open. But

$$f_i^{-1}\big(g^{-1}(W)\big) \;=\; (gf_i)^{-1}(W)$$

and gf_i is continuous by assumption (b). Thus $(gf_i)^{-1}(W) \subseteq X_i$ is an open subset and as this is true for any $i \in I$ we see that $g^{-1}(W) \subseteq Y$ is open. As this is true for any open $W \subseteq Z$ we have found g to be continuous, which is (a).

(ii) Note that $\varrho^{-1}(V) = \{\, x \in X \mid \varrho(x) \in V \,\} = \{\, x \in X \mid [x] \in V \,\}$ such that the quotient topology truly is a special case of a final topology for the single map ϱ only. If $P \subseteq X$ is any subset, then

$$\varrho^{-1}\big(\varrho(P)\big) \;=\; \varrho^{-1}\big(\,\{\,[p] \mid p \in P\,\}\,\big) \;=\; \{\, x \in X \mid \exists\, p \in P : x \in [p] \,\} \;=\; \bigcup_{p\in P} [p]$$

Clearly we have $\varrho([x]) = \{\,[y] \mid y \in [x]\,\} = \{\,[x]\,\}$. And by definition of the quotient topology $\{\,[x]\,\}$ is open, if and only if $\varrho^{-1}(\{\,[x]\,\}) \subseteq X$ is open. But this is $\varrho^{-1}(\{\,[x]\,\}) = \varrho^{-1}(\varrho([x])) =$

$\bigcup \{ [x] \} = [x]$. Hence $\{ [x] \} \subseteq X/\sim$ is open, if and only if $[x] \subseteq X$ is open.

□

Proof of (6.30):
First of all f is well-defined: If $x \in X_i$ and $x \in X_j$ then $x \in X_i \cap X_j$ and hence $f_i(x) = f_j(x)$ by assumption. That is the value $f(x)$ is uniquely determined, and it exists, as the X_i cover X. Further for any subset $B \subseteq Y$ it is clear that

$$\begin{aligned} f^{-1}(B) &= \{ x \in X \mid f(x) \in B \} = \{ x \in X \mid \exists\, i \in I : x_i \in X_i \text{ and } f_i(x) \in B \} \\ &= \bigcup_{i \in I} \{ x \in X_i \mid f_i(x) \in B \} = \bigcup_{i \in I} f_i^{-1}(B) \end{aligned}$$

(i) thus if $V \subseteq Y$ is open, then any $f_i^{-1}(V) \subseteq X_i$ is open, as f_i is continuous. And as $X_i \subseteq X$ is open, too we get that $f_i^{-1}(V) \subseteq X$ is open. Thus the same is true for the union $f^{-1}(V) = \bigcup_i f_i^{-1}(V) \subseteq X$ and hence f is continuous. (ii) if $D \subseteq Y$ is closed then $f_i^{-1}(D) \subseteq X_i$ is closed again, and as $X_i \subseteq X$ is closed this implies, that $f_i^{-1}(D) \subseteq X$ is closed. Therefore the same is true for the *finite* union $f^{-1}(D) = \bigcup_i f_i^{-1}(D) \subseteq X$. Again this means that f is continuous. □

Proof of (6.33):

(i) Clearly $X_i \cap X_i = X_i \subseteq X_i$ is open, and due to property (2) we find (for any $j \neq i$) that $X_i \cap X_j = \emptyset \subseteq X_j$ is open, too. Thus by property (3) $X_i \subseteq X$ is open. Now apply properties (1) and (2) to see that $X \setminus X_i = \bigcup_j X_j \setminus X_i = \bigcup_{j \neq i} X_j$ is open, too and hence $X_i \subseteq X$ also is closed.

(ii) (a) $\Longrightarrow$ (b): If $X = A \oplus B$, then $X = A \cup B$ and $A \cap B = \emptyset$, by definition of the topological sum. And we have already seen in (i), that A and B are both, open and closed. Now as A and B are closed, this yields $\overline{A} \cap B = A \cap B = \emptyset$ and likewise $A \cap \overline{B} = \emptyset$.

(ii) (b) $\Longrightarrow$ (c): Conversely $X = A \cup B \subseteq \overline{A} \cup B \subseteq X$ implies $X = \overline{A} \cup B$. And as also $\overline{A} \cap B = \emptyset$ this yields $B = X \setminus \overline{A}$ and hence B is open. Interchanging A and B we find, that A is open, too. Next note that $\emptyset \subseteq A \cap B \subseteq \overline{A} \cap B = \emptyset$ implies $A \cap B = \emptyset$. And as $X = A \cup B$ this yields $B = X \setminus A$ and hence B is closed, too. Interchanging A and B again, we find, that A is open and closed, as well.

(ii) (c) $\Longrightarrow$ (a): We only have to verify property (3): If $U \subseteq X$ is open, then $U \cap A \subseteq A$ and $U \cap B \subseteq B$ are open, by definition of the relative topology. Conversely if $U \cap A \subseteq A$ and $U \cap B \subseteq B$ are open then there are open subsets V_A and $V_B \subseteq X$ such that $U \cap A = V_A \cap A$ and $U \cap B = V_B \cap B$. And thereby $U = U \cap X = U \cap (A \cup B) = (U \cap A) \cup (U \cap B) = (V_A \cap A) \cup (V_B \cap B)$. Yet as all of the sets A, B, V_A and V_B are open in X, we find that U is open in X, too.

(iii) If $X = X_1 \oplus X_2$ then by (i) the $X_i \subseteq X$ are open and closed. And by definition of the relative topology this means that $A_i = X_i \cap A \subseteq A$ is open and closed, too. Now $A_1 \cap A_2 \subseteq X_1 \cap X_2 = \emptyset$ is clear. And likewise $A = A \cap X = A \cap (X_1 \cup X_2) = (A \cap X_1) \cup (A \cap X_2) = A_1 \cup A_2$. Thus by (ii) (c) $\Longrightarrow$ (a) we found $A = A_1 \oplus A_2$ again.

(iv) If $Y = Y_1 \oplus Y_2$, then by (i) the $Y_i \subseteq Y$ are open and closed. And as f is continuous, this yields that $X_i = f^{-1}(Y_i) \subseteq X$ is open and closed again. We also find $X = f^{-1}(Y) = f^{-1}(Y_1 \cup Y_2) =$

$f^{-1}(Y_1) \cup f^{-1}(Y_2) = X_1 \cup X_2$. And in complete analogy we also find $\emptyset = f^{-1}(\emptyset) = f^{-1}(Y_1 \cap Y_2) = f^{-1}(Y_1) \cap f^{-1}(Y_2) = X_1 \cap X_2$. Thus by (ii) (c) $\implies$ (a) we get $X = X_1 \oplus X_2$ again.

□

Proof of (6.34):

- (a) $\implies$ (b): If $X = X_1 \oplus X_2$ then by (6.33.(i)) we find, that $X_1 \subseteq X$ is both, open and closed. Thus by assumption (a) we get $X_1 = \emptyset$ or $X_1 = X$. Now it suffices to note that $X_1 = \emptyset$ yields $X_2 = X \setminus X_1 = X$, such that either $X_1 = X$ or $X_2 = X$.
- (b) $\implies$ (c): If $X = A \cup B$ for sume subsets $A, B \subseteq X$ with $\overline{A} \cap B = \emptyset = A \cap \overline{B}$, then by (6.33.(ii)) we get $X = A \oplus B$. Thus by assumption we already have $A = X$ or $B = X$.
- (c) $\implies$ (d): We have to verify $\partial A = \emptyset \implies A \in \{\emptyset, X\}$. Thus assume $\partial A = \emptyset$, that is $A^\circ = \overline{A}$. Then we find that $A^\circ = A = \overline{A}$ from $A^\circ \subseteq A \subseteq \overline{A} = A^\circ$. Hence A is closed (as $A = \overline{A}$) and open (as $A = A^\circ$). Thereby $B := X \setminus A$ is open and closed, as well. Hence $\overline{A} \cap B = A \cap B = \emptyset$ and $A \cap \overline{B} = A \cap B = \emptyset$. And as $X = A \cup B$, is clear the pair (A, B) satisfies the condition in the assumption (c). Thus we get $A = X$ or $B = X$. But now it suffices to note that $B = X$ implies $A = X \setminus B = \emptyset$. Thus we have either $A = X$ or $A = \emptyset$, as claimed.
- (d) $\implies$ (a): suppose $A \subseteq X$ is both, open and closed. Then we find $A^\circ = A = \overline{A}$ and hence $\partial A = \emptyset$. By assumption (d) this means $A \in \{\emptyset, X\}$, which had to be shown.

□

Proof of (6.35):

(i) In order to have a precise notation let $\mathrm{cl}_X(A)$ denote the closure of A in the topology of X and $\mathrm{cl}_C(A \cap C)$ the closure of $A \cap C$ in the relative topology of C. We have seen in (6.16.(x)) that $\mathrm{cl}_C(A \cap C) = \mathrm{cl}_X(A \cap C) \cap C$ and hence we get $\mathrm{cl}_C(A \cap C) \subseteq \mathrm{cl}_X(A) \cap C \subseteq \mathrm{cl}_X(A)$ such that

$$\mathrm{cl}_C(C \cap A) \cap (C \cap B) \subseteq \mathrm{cl}_X(A) \cap B \cap C = \emptyset$$

and hence $\overline{(C \cap A)} \cap (C \cap B) = \emptyset$ (where the closure now refers to the relative topology of C). Repeating the argument with B instead of A, we find $(C \cap A) \cap \overline{(C \cap B)} = \emptyset$. But as $C \subseteq A \cap B$ we clearly have $C = (C \cap A) \cup (C \cap B)$. Thus by property (c) of the connected set C we have $C \cap A = C$ or $C \cap B = C$. But this means nothing but $C \subseteq A$ or $C \subseteq B$, which had to be shown.

(iii) We will prove that $S := \bigcup \mathcal{C}$ is connected by verifying property (c) of connected sets. Thus assume we had some subsets $A, B \subseteq S$ such that $S = A \cup B$ and $\mathrm{cl}_S(A) \cap B = \emptyset = A \cap \mathrm{cl}_S(B)$ (where the subscript S denotes that the closure is taken in S). Now recall that $\mathrm{cl}_S(A) = \mathrm{cl}_X(A) \cap S$. Thus for any $C \in \mathcal{C}$ we have $\mathrm{cl}_X(A) \cap B \cap C \subseteq \mathrm{cl}_X(A) \cap B \cap S = \mathrm{cl}_S(A) \cap B = \emptyset$ and likewise $A \cap \mathrm{cl}_X(B) \cap C = \emptyset$. As $C \subseteq S = A \cup B$ (i) now implies $C \subseteq A$ or $C \subseteq B$. Now fix some $C \in \mathcal{C}$, where we assume $C \subseteq A$ without loss of generality. In particular $\mathrm{cl}_X(C) \subseteq \mathrm{cl}_X(A)$ and as $B \subseteq S$ we hence get $\mathrm{cl}_X(C) \cap B \subseteq \mathrm{cl}_X(A) \cap B = \mathrm{cl}_X(A) \cap B \cap S = \mathrm{cl}_S(A) \cap B$. Suppose we had $D \subseteq B$ for some other $D \in \mathcal{C}$, then $\emptyset \neq \bigcap \mathcal{C} \subseteq C \cap D \subseteq \mathrm{cl}_X(C) \cap D \subseteq \mathrm{cl}_X(C) \cap B \subseteq \mathrm{cl}_S(A) \cap B = \emptyset$, a contradiction. Thus we found $D \subseteq A$, as well and as D has been arbitrary this yields $S = \bigcup \mathcal{C} \subseteq A \subseteq S$ and hence $S = A$. Thus S is connected again. And clearly (ii) is a special case of (iii), considering $\mathcal{C} := \{C, D\}$.

(iv) Consider any partition of A into a topological sum $A = A_1 \oplus A_2$ and let us denote $C_i := A_i \cap C$. Then by (6.33.(iii)) we find that $C = C_1 \oplus C_2$. Yet as C was assumed to be connected this implies $C_1 = \emptyset$ or $C_2 = \emptyset$. Without loss of generality we regard the case $C_1 = \emptyset$ only. As $C \subseteq A = A_1 \cup A_2$ this implies $C \subseteq A_2$ and hence $A_1 \subseteq A \subseteq \overline{C} \subseteq \overline{A}_2$. Hence $A_1 = A_1 \cap \overline{A}_2 = A_1 \cap \overline{A}_2 \cap A = A_1 \cap \overline{A}_{2,A} = A_1 \cap A_2 = \emptyset$ (where $\overline{A}_{2,A}$ denotes the closure of A_2 in A, which is A_2 again, as $A_2 \subseteq A$ is closed). Thus we have proved $A_1 = \emptyset$ and hence $A_2 = X$. And as the partition has been arbitrary this means, that A is connected, again.

(v) Suppose $f(C)$ was *not* connected, then by property (b) there are some subsets $F_1, F_2 \subseteq f(C)$ such that $f(C) = F_1 \oplus F_2$ and $F_1, F_2 \neq \emptyset$. Now regard $f : C \to f(C)$, which is a continuous function again and let $C_i := (f\big|_C)^{-1}(F_i) = f^{-1}(F_i) \cap C$. Then by (6.33.(iv)) we find $C = C_1 \oplus C_2$ and as C is connected this implies $C_1 = \emptyset$ or $C_2 = \emptyset$. But on the other hand $F_i \neq \emptyset$ is non-empty, there is some $y_i \in F_i \subseteq f(C)$ and hence some $x_i \in C$ such that $f(x_i) = y_i$. Now $x_i \in C_i$ is clear and hence $C_i \neq \emptyset$ is non-empty, as well. Thus we have obtained a contradiction, which can only be evaded if $f(C)$ is connected.

□

Proof of (6.36):

- We will first prove that $\sim$ truly is an equivalence relation. *Reflexivity*: for any $x \in X$ the set $\{ x \}$ clearly is connected, as the trivial subsets $\emptyset$ and $\{ x \}$ are the only subsets of $\{ x \}$ available. Now $\{ x, x \} \subseteq \{ x \}$ implies $x \sim x$. *Symmetry*: If $x \sim y$, then by definition there is some connected set $C \subseteq X$, such that $\{ x, y \} \subseteq C$. But as $\{ y, x \} = \{ x, y \} \subseteq C$ this already implies $y \sim x$. *Transitivity*: If $x \sim y$ and $y \sim z$ then there are connected sets $C, D \subseteq X$ such that $\{ x, y \} \subseteq C$ and $\{ y, z \} \subseteq D$. Hence $y \in C \cap D$ such that by (6.35.(ii)) $C \cap D$ is connected again. Now, as $\{ x, z \} \subseteq C \cap D$, this yields $x \sim z$.

- It remains to verify that $[x] = \bigcup \{ C \subseteq X \text{ connected} \mid x \in C \}$. For "$\supseteq$" we are given any connected set $C \subseteq X$ such that $x \in C$ and need to verify, that $C \subseteq [x]$. Thus consider any $y \in C$, then $\{ x, y \} \subseteq C$ and hence $x \sim y$, which translates into $y \in [x]$ again. As y has been arbitrary, we truly have $C \subseteq [x]$. Conversely for "$\subseteq$" consider any $y \in [x]$. That is $x \sim y$ and hence there is some connected set $C \subseteq X$ such that $\{ x, y \} \subseteq C$. In particular $x \in C$ and hence $C \in \{ C \subseteq X \text{ connected} \mid x \in C \}$. And as $y \in C$ (and y has been arbitrary) this yields the converse inclusion.

□

Proof of (6.37):

(i) Let us first prove that a connected component $K = \mathrm{cnc}(x)$ is connected [we would speak of a poor name choice, if this was not the case]: Let $\mathcal{C}(x) := \{ C \subseteq X \mid C \text{ connected}, x \in C \}$, then $\{ x \} \in \mathcal{C}(x)$ and $x \in \bigcap \mathcal{C}(x)$. Thus $\mathcal{C}(x)$ is non-empty and has non-empty intersection, such that (6.35.(iii)) tells us, that $\bigcup \mathcal{C}$ is connected again. And by (6.36) we already know $K = \bigcup \mathcal{C}(x)$. We have to postpone the proof, that K already is closed.

(ii) "$\subseteq$": Suppose $K = \mathrm{cnc}(x)$ is a connected component of X, then we need to show that K is maximal among the connected subsets of X. By (i) we know, that K is connected, so it remains to show the

maximality of E: Suppose $K \subseteq C$ for some $C \subseteq X$ connected and consider $y \in C$. Then (as also $x \in C$) $\{x,y\} \subseteq C$ and as C is connected this implies $x \sim y$ and hence $y \in [x] = K$. Thus as y has been arbitrary we found $C \subseteq K$, too and hence $C = K$, which is the maximality of K.

(ii) "$\supseteq$": Conversely suppose K is maximal among the connected subsets of X, then we need to show, that K is a connected component. If $K = \emptyset$, then already $X = \emptyset$ (as for any $x \in X$ the set $\{x\}$ would be a connected set truly larger than $K = \emptyset$) in contradiction to the assumption. Thus there is some element $x \in K$. Next we will show

$$K \;=\; \mathrm{cnc}(x)$$

in particular K is a connected component. The inclusion $K \subseteq \mathrm{cnc}(x)$ is easy: If $y \in K$ then $\{x,y\} \subseteq K$ and as K is connected, this means $x \sim y$ and hence $y \in [x] = \mathrm{cnc}(x)$. Conversely consider any element $y \in \mathrm{cnc}(x)$, that is $x \sim y$ and hence there is some connected set $C \subseteq X$ such that $\{x,y\} \subseteq C$. Hence $x \in C \cap K$ and as both C and K are connected, so is $C \cup K$, according to (6.35.(ii)). But as K was assumed to be maximal and $K \subseteq C \cup K$ is clear, we get $K = K \cup C$, which is $C \subseteq K$. In particular $y \in C \subseteq K$ yields $y \in K$.

(i) Now we are ready to prove that the connected components also are closed: Let $K = \mathrm{cnc}(x)$ be a connected component again. As $K \subseteq \overline{K} \subseteq \overline{K}$ (6.35.(iv)) implies that $\overline{K}$ is connected again. Now combining $K \subseteq \overline{K}$ with the maximality of K we find $K = \overline{E}$, that is K is closed, as well.

(iii) By assumption we have $X \neq \emptyset$. If $C = \emptyset$ then we choose some arbitrary $x \in X$ and let $K := \mathrm{cnc}(x)$. Then K is a connected component and $C \subseteq K$ is clear. Thus we may continue with the case $C \neq \emptyset$. Then we regard the set

$$\mathcal{Z} \;:=\; \{\, D \subseteq X \mid D \text{ connected, } C \subseteq D \,\}$$

As C is connected we have $C \subseteq \mathcal{Z}$ and hence $\mathcal{Z} \neq \emptyset$. Clearly $\mathcal{Z}$ is partially ordered under "$\subseteq$". To apply the lemma of Zorn we have to regard a chain $(D_i) \subseteq \mathcal{Z}$ (where $i \in I$) and find an upper bound for it. Of course our candidate for an upper bound is

$$D \;:=\; \bigcup_{i \in I} D_i$$

Clearly $C \subseteq D_i \subseteq D$ for any $i \in I$ and hence we have to show that D is connected again. Thus consider some decomposition of D as a topological sum $D = D' \oplus D''$. For any $i \in I$ let us denote $D'_i := D_i \cap D'$ and $D''_i := D_i \cap D''$. Then by (6.33.(iii)) we get $D_i = D'_i \oplus D''_i$ again. Yet as the D_i are connected this implies $D'_i = D_i$ or $D''_i = D_i$. Suppose there were some i, $j \in I$ such that $D'_i = D_i$ and $D''_j = D_j$. As (D_i) is a chain we may assume $D_i \subseteq D_j$. Therefore $D_i = D'_i = D_i \cap D' \subseteq D_j \cap D' = D'_j = D_j \setminus D''_j = \emptyset$. That is $D_i = \emptyset$, which cannot be, as $\emptyset \neq C \subseteq D_i$. Thus all the D_i are either equal to D'_i or to D''_i and they all agree which of the two cases is satisfied. Without loss of generality we may assume $D_i = D'_i$ for any $i \in I$. Now $D = \bigcup_i D_i = \bigcup_i D'_i = \bigcup_i D_i \cap D' = D \cap D' = D'$. And as the decomposition has been arbitrary this proves, that D is connected again. Thus by the lemma of Zorn, there is a maximal element $K \in \mathcal{Z}$. And by (ii) it is clear, that any such is a connected component of X. Thus it remains to verify

the uniqueness of K. Suppose $C \subseteq K$ and $C \subseteq L$ for some connected components $K = \text{CNC}(x)$ and $L = \text{CNC}(z)$ and choose any $y \in C$. As $\{x,y\} \subseteq K$ we have $x \sim y$ and likewise $y \sim z$, as $\{y,z\} \subseteq L$. Thus $x \sim z$ and this means $K = [x] = [y] = L$.

(iv) As $\sim$ is an equivalence relation the K_i partition X, that is we have $X = K_1 \cup \cdots \cup K_n$ and $K_i \cap K_j = \emptyset$ for any $i \neq j \in 1 \ldots n$. As we have seen in (i) any $K_i \subseteq X$ is closed. But as the K_i partition X we have $X \setminus K_i = \bigcup_{j \neq i} K_j$, which is a closed set. Thus all of the $K_i \subseteq X$ are open, too. Using (6.33.(ii)) (and induction on n) we finally find the claim $X = K_1 \oplus \cdots \oplus K_n$.

□

Proof of (6.39):

- Let us prove the equivalence of (a) and (c) first: Consider any subset $P \subseteq G$ then $\lambda_x^{-1}(P) = \{ y \in G \mid xy \in P \} = \{ y \in G \mid y \in x^{-1}P \} = x^{-1}P$. Thus if for any $x \in G$ the map λ_x is continuous, then $\lambda_{x^{-1}}$ is continuous, too. So if $U \subseteq G$ is open, then $\lambda_{x^{-1}}^{-1}(U) = xU \subseteq G$ is open, too. Conversely if for any $x \in G$ the coset $xU \subseteq G$ is open, then the same is true for $x^{-1}U = \lambda_x^{-1}(U)$. And this means λ_x is continuous. The same reasoning shows the equivalence of μ_y being continuous and Uy being open again (for any $y \in G$).

- The equivalence of (a) and (d) follows in the same way: Note that λ_x is continuous, iff for any closed set $C \subseteq G$ the preimage $\lambda_x^{-1}(C) = x^{-1}C \subseteq G$ is closed again. Hence if for any $x \in G$ the map λ_x is continuous, then $\lambda_{x^{-1}}$ is continuous, too. So if $C \subseteq G$ is closed, then $\lambda_{x^{-1}}^{-1}(C) = xC \subseteq G$ is closed, too. Conversely if for any $x \in G$ the coset $xC \subseteq G$ is closed, then the same is true for $x^{-1}C = \lambda_x^{-1}(C)$. And this means λ_x is continuous. The same reasoning shows the equivalence of μ_y being continuous and Cy being closed again (for any $y \in G$).

- Now to the equivalence of (b) and (e): By definition $\circ$ is continuous, iff for any $W \subseteq G$ open $\circ^{-1}(W) = \{ (x,y) \in G^2 \mid xy \in W \}$ is an open subset of $G^2 = G \times G$. As G^2 carries the box topology this means that for any $(x,y) \in \circ^{-1}(W)$ there are some $U \in \mathcal{T}(x)$ and $V \in \mathcal{T}(y)$ such that $U \times V \subseteq \circ^{-1}(W)$. Now we replace $(x,y) \in \circ^{-1}(W)$ by "x, $y \in G$ with $xy \in W$" and $U \times V \subseteq W$ by "for any $u \in U$ and $v \in V$ we get $uv \in W$". Then this is statement (e) precisely.

- Now to (b) $\implies$ (a): Fix $x \in G$ and regard the embedding $\iota_x : G \to G^2 : y \mapsto (x,y)$. Let us prove, that this map is continuous, that is if $W \subseteq G^2$ is an open set, then $\iota_x^{-1}(W) = \{ y \in G \mid (x,y) \in W \} \subseteq G$ is open, too. To do this fix any $y \in \iota_x^{-1}(W)$, as $(x,y) \in W$ the definition of the box topology tells us, that there are some $U \in \mathcal{T}(x)$ and $V \in \mathcal{T}(y)$, such that $U \times V \subseteq W$. As $x \in U$ in particular $\iota_x(v) = (x,v) \in W$ for any $v \in V$. And as this is true for any $v \in V$ we have $y \in V \subseteq \iota_y^{-1}(W)$. As we have found such an open set V for any $y \in \iota_y^{-1}(W)$, this means, that $\iota_x^{-1}(W)$ is open, by (6.16.(ix)).

 Now that ι_x is continuous, we note that $\lambda_x(y) = xy = \circ\iota_x(y)$, that is $\lambda_x = \circ\iota_x$ is a composition of continuous maps and hence continuous itself. Analogously $\mu_y = \circ\iota_y$ where $\iota_y(x) := (x,y)$ is continuous, too. For the same reason μ_y is continuous for any $y \in G$.

- We finish by proving (e) $\implies$ (c), that is we regard any $W \subseteq G$ open and need to show that for any x, $y \in G$ the cosets xW and Wy are open again. As this should be true for any x, $y \in G$, let us prove that $x^{-1}W$ and Wy^{-1} are open, instead. If $W = \emptyset$, then $x^{-1}W$ and $Wy^{-1} = \emptyset$ which

is open. So we consider $W \neq \emptyset$ and fix any $x \in G$ and $y \in x^{-1}W$. That is $xy \in W$ and hence, by assumption (e), there are some $U \in \mathcal{T}(x)$ and $V \subseteq \mathcal{T}(y)$ such that for any $u \in U$ and $v \in V$ we have $uv \in W$. In particular for $u = x$ this is $v \in x^{-1}W$. As this is true for any $v \in V$ we have $V \subseteq x^{-1}W$ and $y \in V$. As this is true for any $y \in x^{-1}W$ we know that $x^{-1}W$ is open, by (6.16.(ix)). In the same way it can be seen, that Wy^{-1} is open.

□

Proof of (6.41):

- The first thing to do is check the well-definedness of the metric: Consider any $x, y \in G$ with $x \neq y$ and let $N := \{ k \in \mathbb{N} \mid x - y \in F_k \}$. As $x - y \in G = F_0$ we generally have $0 \in N$, such that N is non-empty. Also, if $m \notin N$, then for any $n \geq m$ we have $F_n \subseteq F_m$ such that $x - y \notin F_m$ also implies $x - y \notin F_n$. Thus $m \notin N$ implies $n \notin N$ for any $n \geq m$. Suppose we had $N = \mathbb{N}$, then $x - y$ would be contained in the intersection $\bigcap_n F_n = \{0\}$. As $x \neq y$ this cannot be and hence there is some $m \in \mathbb{N}$ such that $x - y \notin F_m$. As we have just argued, this implies $n \notin N$ for any $n \geq m$ and thereby $N \subseteq 0 \ldots (m-1)$. In particular N is a finite, non-empty set and thereby it has a maximum.

- Before proving that d is a metric, let us verify that $x + F_m$ is a closed ball of radius 2^{-m}. That is d satisfies the property: $x + F_m = \{ y \in G \mid d(x,y) \leq 2^{-m} \}$. For the inclusion from left to right we start with some $f \in F_m$ and have to show $d(x, x+f) \leq 2^{-m}$. If $f = 0$, then $d(x, x+f) = 0 \leq 2^{-m}$. If $f \neq 0$ we have $d(x, x+f) = 2^{-n}$ where $n = \max\{ k \in \mathbb{N} \mid x - (x+f) \in F_k \}$. Hereby $x - (x+f) = -f \in F_m$, such that m is contained in this set. In particular $n \geq m$ and thereby $d(x, x+f) = 2^{-n} \leq 2^{-m}$. Conversely from right to left, we have $d(x,y) \leq 2^{-m}$. If $x = y$ then $y = x + 0 \in x + F_m$ is granted. If $x \neq y$ let $d(x,y) = 2^{-n}$ where $n = \max\{ k \in \mathbb{N} \mid x - y \in F_k \}$. As $2^{-n} = d(x,y) \leq 2^{-m}$ we have $m \leq n$, in particular $x - y \in F_n \subseteq F_m$. Letting $f := y - x \in F_m$ we get $y = x + f \in x + F_m$.

- Next we check, that d is a metric on G: Clearly $d(x,y) \geq 0$ for any $x, y \in G$, by construction. Also if $x = y$, then $d(x,y) = 0$. Conversely, if $x \neq y$ then $d(x,y) = 2^{-n} > 0$ for some $n \in \mathbb{N}$. Thus (M2) is satisfied, as well. Now to the symmetry: If $x = y$, then $d(x,y) = 0 = d(y,x)$ is clear. In case $x \neq y$ the equality $d(x,y) = 2^{-n}$ means $x - y \in F_n$ but $x - y \notin F_{n+1}$. But F_n and F_{n+1} are subgroups, so $x - y \in F_n$ is equivalent to $y - x \in F_n$. Likewise $x - y \notin F_{n+1}$ is equivalent to $y - x \notin F_{n+1}$. Thus we get $d(y,x) = 2^{-n} = d(x,y)$. It remains to prove the triangle inequality: Consider any $x, y, z \in G$. If $y = x$ then $d(x,z) = d(y,z) = d(x,y) + d(y,z)$, likewise $d(x,z) = d(x,y) = d(x,y) + d(y,z)$ in case $y = z$. So let us assume $y \notin \{ x, z \}$. Then we have $d(x,y) = 2^{-m}$ and $d(y,z) = 2^{-n}$ for some maximal $m, n \in \mathbb{N}$ with $x - y \in F_m$ and $y - z \in F_n$. Without loss of generality let $m \leq n$, else interchange x and z. Then we have $F_n \subseteq F_m$ and hence, as F_m is a subgroup, $x - z = (x - y) + (y - z) \in F_m$. In particular $d(x,y) \leq 2^{-m} < 2^{-m} + 2^{-n} = d(x,y) + d(y,z)$.

- The equivalence of the open sets is easy: (a) $\iff$ (b) is just the definition of an open set, in a metric space. And we have already seen $B_{1/2^n}(x) \subseteq x + F_n \subseteq B_r(x)$ for any $r > 1/2^n$ in the second item, above. Thus for (c) $\implies$ (b) choose $r := 1/2^n > 0$, then $B_r(x) \subseteq x + F_n(x) \subseteq U$. Conversely for (b) $\implies$ (c) simply choose some $n \in \mathbb{N}$ such that $2^{-n} < r$. Then $x + F_n \subseteq B_r(x) \subseteq U$ such that $x \in x + F_n \subseteq U$ is satisfied, as well.

- It only remains that $(G, \mathcal{T}, +)$ is a topological group. That is for any open set $U \subseteq G$ and any $x \in G$ we have to verify, that $x + U$, $U + x$ and $-U = \{ -u \mid u \in U \}$ are open again. As G is commutative we have $x + U = U + x$ and hence it suffices to check $x + U \subseteq G$ open. So consider any $y \in x + U$, that is $y - x \in U$. As U is open, property (c) asserts, that there is some $n \in \mathbb{N}$, such that $(y - x) + F_n \subseteq U$. Adding x to this equation we get $y + F_n \subseteq x + U$ and as this is true for any $y \in x + U$ we find, that $x + U$ is open, again. Likewise we start with any $y \in -U$, which is $-y \in U$. Again, as U is open, there is some $n \in \mathbb{N}$ such that $(-y) + F_n \subseteq U$. Taking inverses, we find $y - F_n = -((-y) + F_n) \subseteq -U$. But $-F_n = F_n$, as F_n is a subgroup, such that we get $y + F_n \subseteq -U$, which means that $-U$ is open, too.

□

Proof of (6.43):

- It is easy to see, that $\sim$ is an equivalence relation on $\text{Cauchy}(X, d)$: If $(x_n) \subseteq X$ is a Caucy-sequence then for any $\varepsilon > 0$ we find some $n(\varepsilon) \in \mathbb{N}$ such that (for any $m = n \geq n(\varepsilon)$) we get $d(x_n, x_n) < \varepsilon$ and this is $(x_n) \sim (x_n)$. The symmetry of $\sim$ is clear, as d is symmetric: If $(x_n) \sim (y_n)$ then $d(y_n, x_n) = d(x_n, y_n) < \varepsilon$, such that $(y_n) \sim (x_n)$, as well. And finally $\sim$ also is transitive: If $(x_n) \sim (y_n)$ and $(y_n) \sim (z_n)$ and $\varepsilon > 0$ is given, then we can choose $n(\varepsilon) \in \mathbb{N}$ such that $d(x_n, y_n) < \varepsilon/2$ and $d(y_n, z_n) < \varepsilon/2$ and thereby $d(x_n, z_n) \leq d(x_n, y_n) + d(y_n, z_n) < \varepsilon/2 + \varepsilon/2 = \varepsilon$ which means $(x_n) \sim (z_n)$ again.

- Let us first prove, that for any (x_n) and $(y_n) \in \text{Cauchy}(X, d)$ the sequence $(d_n) := (d(x_n, y_n)) \subseteq \mathbb{R}$ truly converges. As $\mathbb{R}$ is complete, it suffices to check, that (d_n) is a Cauchy-sequence. But (x_n) and (y_n) are, so given any $\varepsilon > 0$ we choose $n(\varepsilon) \in \mathbb{N}$, such that for any m, $n \geq n(\varepsilon)$ we have $d(x_m, x_n) < \varepsilon/2$ and $d(y_m, y_n) < \varepsilon/2$. Now let us compute

$$\begin{aligned} d(x_n, y_n) - d(x_m, y_m) &\leq d(x_n, x_m) + d(x_m, y_n) - d(x_m, y_m) \\ &\leq d(x_n, x_m) + d(x_m, y_m) + d(y_m, y_n) - d(x_m, y_m) \\ &= d(x_n, x_m) + d(x_m, y_n) \\ &< \varepsilon/2 + \varepsilon/2 \; = \; \varepsilon \end{aligned}$$

 Interchanging m and n, we find $-(d(x_n, y_n) - d(x_m, y_m)) = d(x_m, y_m) - d(x_n, y_n) < \varepsilon$, as well, such that $|d_n - d_m| = |d(x_n, y_n) - d(x_m, y_m)| < \varepsilon$. But this is the metric of $\mathbb{R}$, such that $(d_n) \subseteq \mathbb{R}$ is a Cauchy-sequence and hence convergent.

- In the next step, we will prove, that $\widehat{d}$ is well-defined: That is if $(x_n) \sim (x'_n)$ and $(y_n) \sim (y'_n)$ are Cauchy-sequences, then we have to check, that $d(x_n, y_n)$ and $d(x'_n, y'_n)$ converge to the same limit. And this can be done by proving that the difference converges to 0. So let's take a look: Given any $\varepsilon > 0$ we can choose $n(\varepsilon) \in \mathbb{N}$ in such a way that for any $n \geq n(\varepsilon)$ we get $d(x_n, x'_n) < \varepsilon/2$ and $d(y_n, y'_n) < \varepsilon/2$ and with this we may compute

$$\begin{aligned} d(x_n, y_n) - d(x'_n, y'_n) &\leq d(x_n, x'_n) + d(x'_n, y_n) - d(x'_n, y'_n) \\ &\leq d(x_n, x'_n) + d(x'_n, y'_n) + d(y'_n, y_n) - d(x'_n, y'_n) \\ &= d(x_n, x'_n) + d(y'_n, y_n) \end{aligned}$$

$$< \quad \varepsilon/2+\varepsilon/2 \;=\; \varepsilon$$

Interchanging x_n with x'_n and y_n with y'_n respectively, we also see $-(d(x_n,y_n)-d(x'_n,y'_n)) = d(x'_n,y'_n)-d(x_n,y_n) < \varepsilon$ and hence $|d(x_n,y_n)-d(x'_n,y'_n)| < \varepsilon$. As this is the metric of $\mathbb{R}$ we conclude $(d(x_n,y_n)-d(x'_n,y'_n)) \to 0$ which means that $(d(x_n,y_n))$ and $(d(x'_n,y'_n)) \subseteq \mathbb{R}$ converge to the same limit. And this means that $\widehat{d}$ is independent of the specific representative of $[x_n]$ resp. $[y_n]$ chosen.

- Let us now prove, that for any x, $y \in X$ we get $\widehat{d}([x],[y]) = d(x,y)$. That is $(d(x_n,y_n)) \to d(x,y)$. But by construction $x_n = x$ and $y_n = y$ for any $n \in \mathbb{N}$, such that $(d(x_n,y_n))$ is the constant sequence $(d(x,y))$. And for this it is clear, that it converges against $d(x,y)$.

- Let us check, that $\widehat{d}$ is a metric: First of all, as for any (x_n), $(y_n) \in \text{Cauchy}\,(X,d)$ and any $n \in \mathbb{N}$ we have $d_n := d(x_n,y_n) \geq$ the limit of $(d_n) \subseteq \mathbb{R}$ has to be positive, too. That is we always get $\widehat{d}([x_n],[y_n]) \geq 0$.

 Next we note that $\widehat{d}([x_n],[y_n]) = 0$ is equivalent to $(d(x_n,y_n)) \to 0$ which means that for any $\varepsilon > 0$ there is some $n(\varepsilon) \in \mathbb{N}$, such that $0 \geq d(x_n,y_n) < \varepsilon$. But this is precisely the definition of $(x_n) \sim (y_n)$ such that $[x_n] = [y_n]$. Thus $\widehat{d}$ also is definite.

 And clearly $\widehat{d}$ is symmetric, as d is symmetric. It only remains to verify the triangle inequality $\widehat{d}([x_n],[z_n]) \leq \widehat{d}([x_n],[y_n]) + \widehat{d}([y_n],[z_n])$. So look into the defining sequences, $\widehat{d}([x_n],[z_n])$ is the limit of $d(x_n,z_n)$ and by the triangle inequality of d we have $d(x_n,z_n) \leq d(x_n,y_n)+d(y_n,z_n)$. By taking $n \to \infty$ we find

$$\begin{aligned}\widehat{d}\big([x_n],[z_n]\big) \;&=\; \lim_{n\to\infty} d(x_n,z_n) \;\leq\; \lim_{n\to\infty}\big(d(x_n,y_n)+d(y_n,z_n)\big)\\ &=\; \lim_{n\to\infty} d(x_n,y_n) + \lim_{n\to\infty} d(y_n,z_n) \;=\; \widehat{d}\big([x_n],[y_n]\big)+\widehat{d}\big([y_n],[z_n]\big)\end{aligned}$$

- The next claim is that the natural map $\kappa : X \hookrightarrow \widehat{X} : x \mapsto [x]$ is injective: So consider any two x, $y \in X$ such that $[x] = [y]$. We have already seen, that this implies $0 = \widehat{d}([x],[y]) = d(x,y)$ such that we find $x = y$.

- But κ also is continuous, as both (X,d) and $(\widehat{X},\widehat{d})$ are metric spaces, we can use (6.6) by which it suffices to show, that for any $x \in X$ and $\varepsilon > 0$ there is some $\delta > 0$ such that $u \in B_\delta(X,x)$ implies $[u] \in B_\varepsilon(\widehat{X},[x])$. But we can just take $\delta := \varepsilon$ as thereby $\widehat{d}([u],[x]) = d(u,x) < \varepsilon$.

- Let us now prove that the completion $\widehat{X}$ is just that - complete. That is we are given a Cauchy-sequence $(s_m) \subseteq \widehat{X}$ and need to construct some $s \in \widehat{X}$ such that $(s_m) \to s$. As (s_m) is a Cauchy-sequence for any $\varepsilon > 0$ there is some $m(\varepsilon) \in \mathbb{N}$ such that for any m, $n \geq m(\varepsilon)$ we get $\widehat{d}(s_m,s_n) < \varepsilon/2$. And by construction any s_m is of the form $s_m = [x_{m,k}]$ for a Cauchy-sequence $(x_{m,k})$ (where the index runs over $k \in \mathbb{N}$). By definition of $\widehat{d}$ this is

$$\widehat{d}(s_m,s_n) \;=\; \lim_{k\to\infty} d\big(x_{m,k},x_{n,k}\big) \;<\; \frac{\varepsilon}{2}$$

 As $d(x_{m,k},x_{n,k})$ converges to $\widehat{d}(s_m,s_n)$ for any $\varepsilon > 0$ there is some $k(\varepsilon) \in \mathbb{N}$ such that for any

$k \geq k(\varepsilon)$ we get $|d(x_{m,k}, x_{n,k}) - \widehat{d}(s_m, s_n)| < \varepsilon/2$. Together this means

$$d(x_{m,k}, x_{n,k}) \;<\; \frac{\varepsilon}{2} + \widehat{d}(s_m, s_n) \;<\; \frac{\varepsilon}{2} + \frac{\varepsilon}{2} \;=\; \varepsilon$$

Now let $n(\varepsilon) := \max\{\, m(\varepsilon), k(\varepsilon) \,\}$ and for any $k \in \mathbb{N}$ we let $x_k := (x_{k,k})$ the diagonal elements of the s_k. Then, by the above, we have the following estimate for any m, $k \geq n(\varepsilon)$

$$d(x_{m,k}, x_k) \;=\; d(x_{m,k}, x_{k,k}) \;<\; \varepsilon$$

In particular, for any $m \geq n(\varepsilon)$ we see that the limit of $d(x_{m,k}, x_k)$ for $k \to \infty$ is ε at most. But the limit of this sequence is

$$\widehat{d}(s_m, s) \;=\; \lim_{k\to\infty} d(x_{m,k}, x_k) \;\leq\; \varepsilon$$

and as this is true for any $m \geq n(\varepsilon)$ we have found $(s_m) \to s$ for $m \to \infty$. In short: The diagonal sequence $(x_{k,k})$ yields the desired limit. And thereby $(x_{k,k})$ is a Cauchy-sequence in X, as for any j, $k \geq n(\varepsilon)$ we have seen $d(x_j, x_k) < \varepsilon$ before. That is the limit $s = [x_k] \in \widehat{X}$ is a well-defined point in the completion.

- In a final step we need to verify, that $\kappa(X)$ is a dense subset of $\widehat{X}$. But by (6.21.(v)) the closure of $\kappa(X)$ is given to be the set of limits of convergent sequences in $\kappa(X)$. So if we start with any $s := [x_n] \in \widehat{X}$ we need to find a sequence $(s_n) \in \kappa(X)$, such that $(s_n) \to s$. But this can be done in the following way: For any $n \in \mathbb{N}$ let $s_n := [x_n]$ for the *fixed* $x_n \in X$. As $(x_n) \subseteq X$ is a Cauchy-sequence we get: For any $\varepsilon > 0$ there is some $n(\varepsilon) \in \mathbb{N}$ such that for any m, $n \geq n(\varepsilon)$ we get $d(x_m, x_n) < \varepsilon/2$. Let us use this, to prove $(s_n) \to s$: The m-th coefficient of s_n is x_n, whereas the m-th coefficient of s is x_m. Thus $\widehat{d}(s_n, s)$ is the limit of $d(x_n, x_m)$ for $m \to \infty$. And by construction we have $d(x_n, x_m) < \varepsilon/2$ for any m, $n \geq n(\varepsilon)$. By taking to the limit $m \to \infty$ we find $\widehat{d}(s_n, s) \leq \varepsilon/2 < \varepsilon$ for any $n \geq n(\varepsilon)$. And this is precisely what we needed for $(s_n) \to s = [x_n]$. And as $[x_n] \in \widehat{X}$ was arbitrary, this means that $\widehat{X}$ is contained in the closure of $\kappa(X)$, such that the closure must be equal to $\widehat{X}$.

□

15.8 Proofs of Chapter 7

Proof of (7.2):
Throughout this proof we assume α, γ, $\varepsilon \in A$ and β, δ, $\eta \in B$. Suppose A and B are integral and $(\alpha,\beta)+(\varepsilon,\eta) = (\gamma,\delta)+(\varepsilon,\eta)$. By construction this means $\alpha+\varepsilon = \gamma+\varepsilon$ and $\beta+\eta = \delta+\eta$. But if A and B are integral this impliea $\alpha = \gamma$ and $\beta = \delta$ which is $(\alpha,\beta) = (\gamma,\delta)$ again. Hence in this case $A \times B$ is integral, too.
For any $\varepsilon \in A$ let us denote $S_A^{-1}(\varepsilon) := \{\, (\alpha,\gamma) \in A^2 \mid \alpha+\gamma = \varepsilon \,\}$ and likewise $S_B^{-1}(\eta)$ for some $\eta \in B$. Then $((\alpha,\beta),(\gamma,\delta)) \in S_{A\times B}^{-1}(\varepsilon,\eta)$ is equivalent to $(\alpha+\gamma,\beta+\delta) = (\varepsilon,\eta)$ which in turn is equivalent to $(\alpha,\gamma) \in S_A^{-1}(\varepsilon)$ and $(\beta,\delta) \in S_B^{-1}(\eta)$. That is we have a bijection of

$$\begin{array}{rcl} S_{A\times B}^{-1}(\varepsilon,\eta) & \longleftrightarrow & S_A^{-1}(\varepsilon) \times S_B^{-1}(\eta) \\ \big((\alpha,\beta),(\gamma,\delta)\big) & \mapsto & \big((\alpha,\gamma),(\beta,\delta)\big) \end{array}$$

If A and B are solution-finite, then both $S_A^{-1}(\varepsilon)$ and $S_B^{-1}(\eta)$ are finite and hence $S_A^{-1}(\varepsilon) \times S_B^{-1}(\eta)$ is finite, as well. But this means in this case $A \times B$ is solution-finite, too. □

Proof of (7.6):

(i) Recall the definition of the *minimum* and *maximum* of any two elements $\alpha,\beta \in A$ (this is truly well-defined, since $\leq$ is a linear order)

$$\alpha \wedge \beta \;:=\; \begin{cases} \alpha \text{ if } \alpha \leq \beta \\ \beta \text{ if } \beta \leq \alpha \end{cases} \qquad \alpha \vee \beta \;:=\; \begin{cases} \beta \text{ if } \alpha \leq \alpha \\ \beta \text{ if } \beta \leq \alpha \end{cases}$$

In the case that $M = \{\, \mu \,\}$ contains one element only, we clearly get the minimal and maximal elements $\mu_* = \mu = \mu^*$. If now M is given to be $M = \{\, \mu_1,\ldots,\mu_n \,\}$ where $n \geq 2$ then we regard

$$\begin{array}{rcl} \mu_* & := & (\ldots(\mu_1 \wedge \mu_2)\ldots) \wedge \mu_n \\ \mu^* & := & (\ldots(\mu_1 \vee \mu_2)\ldots) \vee \mu_n \end{array}$$

Then μ_* and μ^* are minimal, resp. maximal elements of M, which can be seen by induction on n: if $n = 2$ then μ_* is minimal by construction. Thus for $n \geq 3$ we let $H := \{\, \mu_1,\ldots,\mu_{n-1} \,\} \subseteq M$. By induction hypothesis we have $H_* = \{\, \nu_* \,\}$ for $\nu^* = ((\mu_1 \wedge \mu_2)\ldots) \wedge \mu_{n-1}$. Now let $\mu_* := \nu_* \wedge \mu_n$ then $\mu_* \leq \nu_* \leq \mu_i$ for $i < n$ and $\mu_* \leq \mu_n$ by construction. Hence we have $\mu_* \leq \mu_i$ for any $i \in 1\ldots n$, which means $\mu_* \in M_*$. And the uniqueness is obvious by the anti-symmetry of $\leq$. And this also proves the the claim for the maximal element μ^*, by taking to the inverse order $\alpha \geq \beta \;:\Longleftrightarrow\; \beta \leq \alpha$.

(ii) The existence of μ_* is precisely the property of a well-ordering. The uniqueness is immediate from the anti-symmetry of $\leq$ again: suppose μ_1 and μ_2 both are minimal elements of M, in particular $\mu_1 \leq \mu_2$ and $\mu_2 \leq \mu_1$. And this implies $\mu_1 = \mu_2$, as $\leq$ is a (linear) order on A.

(iii) In the direction (a) $\Longrightarrow$ (b) we consider $\alpha < \beta$. By the positivity of $\leq$ this implies $\alpha+\gamma \leq \beta+\gamma$. If the equality $\alpha+\gamma = \beta+\gamma$ would hold true then - as A is integral - we would find $\alpha = \beta$ in contradiction to the assumption $\alpha < \beta$. In the converse direction (b) $\Longrightarrow$ (a) we are given $\alpha \leq \beta$.

The positivity $\alpha + \gamma \leq \beta + \gamma$ (for any $\gamma \in A$) of $\leq$ is clear in this case. Now asume $\alpha + \gamma = \beta + \gamma$ then we need to show $\alpha = \beta$ to see that A is integral. But as $\leq$ is total we have $\alpha \leq \beta$ or $\beta \leq \alpha$, where we may assume $\alpha \leq \beta$ without loss of generality. If we now had $\alpha \neq \beta$ then $\alpha < \beta$ and hence $\alpha + \gamma < \beta + \gamma$ in contradiction to $\alpha + \gamma = \beta + \gamma$, which rests this case, too. Now (c) $\implies$ (b) is trivial such that there only remains the direction (b) $\implies$ (c). But this is clear - assume $\alpha + \gamma < \beta + \gamma$ but $\alpha \geq \beta$, then by the positivity (a) we would get the contradiction: $\alpha + \gamma \geq \beta + \gamma$.

(vii) We only need to show that $\geq$ is (strictly) positive again. That is we are given some α, α' and $\beta \in A$ such that $\alpha \geq \alpha'$ and we need to show $\alpha + \beta \geq \alpha' + \beta$. By definition this means $\alpha' \leq \alpha$. And as $\leq$ is (strictly) positive this implies $\alpha' + \beta \leq \alpha + \beta$ which again turns into $\alpha + \beta \geq \alpha' + \beta$. In the "strict" case all we have to do is replace "$\leq$" by "$<$" and likewise "$\geq$" by "$>$". Alternatively we could argue, that the integral property does not depend on the ordering chosen.

(iv) Assume $\mu \neq \mu_*$, then by minimality of μ_* this would yield $\mu_* < \mu$ and hence (by property (b) in item (iii) above) $\mu + \nu = \mu_* + \nu_* < \mu + \nu_*$. Thus we see that $\nu \neq \nu_*$ and hence (by minimality of ν_*) we get $\nu_* < \nu$ again. Using (b) once more this yields a contradiction

$$\mu + \nu \;<\; \mu + \nu_* \;<\; \mu + \nu$$

Thus we have seen that $\mu + \nu = \mu_* + \nu_*$ implies $\mu = \mu_*$ but in complete analogy we find that $\nu \neq \nu_*$ leads to another contradiction and hence $\nu = \nu_*$. The statement for maximal elements could be done in complete analogy to the minimal elements here. However it is even easier to regard the inverse order $\alpha \geq \beta$ which is a strictly positive order on A again, according to (vii). Under this order the maximal elements of $\geq$ are minimal elements of $\leq$. Hence the statement for maximal elements of $\leq$ turns into the statement for minimal elements of $\geq$. As as $\geq$ is a strictly positive, linear order on A again, this has been proved.

(viii) By assumption we have that for any $\gamma \in A$ the set $L_\gamma := \{\, \alpha \in A \mid \alpha \leq \gamma \,\}$ is finite. And we have to show that for any $\gamma \in A$ the set $A_\gamma := \{\, (\alpha, \beta) \in A^2 \mid \alpha + \beta = \gamma \,\}$ is finite, too. By assumption in particular the set L_0 is finite, thus we may take $\nu \in A$ to be the minimum of this set

$$\nu \;:=\; \min\{\, \alpha \in A \mid \alpha \leq 0 \,\}$$

This ν satisfies $\nu \leq \beta$ for any $\beta \in A$: If $\beta \leq 0$, then $\nu \leq \beta$ is just the minimality of ν. And if $\beta > 0$ then $\nu \leq 0 < \beta$ implies $\nu \leq \beta$, as well. Let us use this ν to define the following map

$$A_\beta \;\hookrightarrow\; L_\gamma \;:\; (\alpha, \beta) \mapsto \alpha$$

We first have to prove, that this map is well-defined: If we start with $(\alpha, \beta) \in A_\gamma$, then $\alpha + \beta = \gamma$. But we also have $\nu \leq \beta$ and by adding α this turns into $\alpha + \nu \leq \alpha + \beta = \gamma$ such that $\alpha + \nu \leq \gamma$ as desired. Next we will prove, that this map is injective: That is we start with any two (α, β) and (α', β') such that $\alpha + \beta = \alpha' + \beta'$ and $\alpha + \nu = \alpha' + \nu$. As A is integral, we get $\alpha = \alpha'$ from this. Thereby $\alpha + \beta = \gamma = \alpha + \beta'$ such that $\beta = \beta'$ as A still is integral. Altogether this is $(\alpha, \beta) = (\alpha', \beta')$ the injectivity of this map. Now that we have the injectivity, we conclude $\#A_\gamma \leq \#L_\gamma$ and in particular $\#A_\gamma$ is finite.

(ix) Let $A_0 := \{ (\alpha,\beta) \in A^2 \mid \alpha+\beta = 0 \}$. As A is solution finite we know, that A_0 is finite. Also let $A_+ := \{ \alpha \in A \mid \alpha > 0 \text{ and } \exists\, \beta \in A : \alpha+\beta = 0 \}$. Suppose there was some $\alpha \in A_+$. As A is integral the $\beta \in A$ for which $\alpha+\beta = 0$ is uniquely determined by α. Thus we would find an injective map of the form

$$A_+ \;\hookrightarrow\; A_0 \;:\; \alpha \mapsto (\alpha,\beta)$$

In particular we see that A_+ has to be a finite set. Choose $\mu := \min(A_+)$ the minimal element with this properties and let $\nu \in A$ be its partner $\mu+\nu = 0$. We will now prove that for any $n \geq 1$ we get (1) $n\mu \in A_+$ and (2) $n\mu + n\nu = 0$ and (3) $n\mu < (n+1)\mu$. Of course we will use induction on n and for $n = 1$ we have (1) and (2) by construction. As $\mu \in A_+$ we have $0 < \mu$ and thereby $\mu = 0+\mu < \mu+\mu = 2\mu$ which also is property (3). Now for the induction step: First of all we have $(n+1)\mu + (n+1)\nu = n\mu+\mu+n\nu+\nu = (n\mu+n\mu)+(\mu+\nu) = 0+0 = 0$, which is (2). And as $0 < \mu$ we get $n\mu = 0+n\mu < \mu+n\mu = (n+1)\mu$, which is (3). As $n\mu \in A_+$ by induction hypothesis we have $0 < n\mu$ and in combination with (3) also $0 < (n+1)\mu$. If we combine this with (2) we get $(n+1)\mu \in A_+$ again. Thus the induction is complete and we have found

$$0 \;<\; \mu \;<\; 2\mu \;<\; 3\mu \;<\; \ldots \;\in\; A_+$$

That is we have found infinitely many distinct elements in A_+ which contradicts A_+ being a finite set. The only way to evade this contradiction is by not mapping A_+ into A_0. And this only is the case if $A_+ = \emptyset$. That is there are *no* $\alpha \in A$ with $\alpha > 0$ and $\alpha+\beta = 0$ for some $\beta \in A$. But if $\alpha < 0$ and $\beta < 0$ then we get $\alpha+\beta < 0+\beta = \beta < 0$ such that $\alpha+\beta < 0$. In particular $\alpha+\beta \neq 0$ for all but $\alpha = 0 = \beta$.

□

Proof of (7.7):

- In the following we will regard arbitrary elements $\alpha = (\alpha_i)$, $\beta = (\beta_i)$ and $\gamma = (\gamma_i) \in A := \mathbb{N}^{\oplus I}$. In a first step we will show that - assuming $(I,\leq)$ is a linearly ordered set - the lexicographic order is a positive partial order on A. The *reflexivity* $\alpha \leq_{\text{lex}} \alpha$ is trivial, however, and for the *transitivity* we are given $\alpha \leq_{\text{lex}} \beta$ and $\beta \leq_{\text{lex}} \gamma$ and need to show $\alpha \leq_{\text{lex}} \gamma$. The case where two (or more) of α, β and γ are equal is trivial and hence the assumption $\alpha <_{\text{lex}} \beta <_{\text{lex}} \gamma$ reads as

$$\begin{aligned} \alpha_k < \beta_k \quad &\text{and} \quad \forall\, i < k \;:\; \alpha_i = \beta_i \\ \beta_l < \gamma_l \quad &\text{and} \quad \forall\, i < l \;:\; \beta_i = \gamma_i \end{aligned}$$

for some $k,l \in I$. We now let $m := \min\{k,l\}$ then it is easy to see, that $\forall\, i < m \;:\; \alpha_i = \beta_i = \gamma_i$ and $\alpha_m < \gamma_m$ which establishes $\alpha <_{\text{lex}} \gamma$. It remains to prove the *anti-symmetry*, i.e. we are given $\alpha \leq_{\text{lex}} \beta$ and $\beta \leq_{\text{lex}} \alpha$ and need to show $\alpha = \beta$. Suppose we had $\alpha \neq \beta$ then again

$$\begin{aligned} \alpha_k < \beta_k \quad &\text{and} \quad \forall\, i < k \;:\; \alpha_i = \beta_i \\ \beta_l < \alpha_l \quad &\text{and} \quad \forall\, i < l \;:\; \beta_i = \alpha_i \end{aligned}$$

In the case $k \leq l$ this implies $\alpha_k < \beta_k = \alpha_k$ and in the case $l \leq k$ we get $\beta_l < \alpha_l = \beta_l$. In both cases this is a contradiction. Hence $\leq_{\text{lex}}$ is a partial order, but the *strict positivity* is easy: Assume

$\alpha <_{\text{lex}} \beta$, then we need to show $\alpha + \gamma <_{\text{lex}} \beta + \gamma$. So by assumption there is some $k \in I$ such that

$$\alpha_k < \beta_k \quad \text{and} \quad \forall\, i < k \;:\; \alpha_i = \beta_i$$

But then $\alpha + \gamma <_{\text{lex}} \beta + \gamma$ is clear, as we can simply add $\gamma_k \in \mathbb{N}$ to $\alpha_k < \beta_k$ and add $\gamma_i \in \mathbb{N}$ to any $\alpha_i = \beta_i$ in the above property, from which we find

$$\alpha_k + \gamma_k < \beta_k + \gamma_k \quad \text{and} \quad \forall\, i < k \;:\; \alpha_i + \gamma_i = \beta_i + \gamma_i$$

- In a second step we will show that - assuming $(I, \leq)$ is a well-ordered set - the lexicographic order truly is a positive linear order on A. By the first step it only remains to verify that $\leq_{\text{lex}}$ is *total*, i.e. we assume that $\beta \leq_{\text{lex}} \alpha$ is untrue and need to show $\alpha \leq_{\text{lex}} \beta$. The assumption that $\beta \leq_{\text{lex}} \alpha$ is false means, that for any $k \in I$ we have

$$\beta_k \geq \alpha_k \quad \text{or} \quad \exists\, i < k \;:\; \alpha_i \neq \beta_i$$

It is clear that in particular $\alpha \neq \beta$ and therefore there is some $l \in I$ such that $\alpha_l \neq \beta_l$. Now, as $(I, \leq)$ is a well-ordered set, we may choose

$$k \;:=\; \min\{\, l \in I \mid \alpha_l \neq \beta_l \,\}$$

Then $\forall\, i < k$ we get $\alpha_i = \beta_i$ (as k was chosen minimally) and $\beta_k \geq \alpha_k$ (by assumption). Yet $\beta_k = \alpha_k$ is false by construction which only leaves $\beta_k > \alpha_k$ and hence establishes $\alpha \leq_{\text{lex}} \beta$.

- In the third step we assume that I is finite, i.e. $I = 1 \ldots n$ without loss of generality. Note that I clearly is well-ordered under its standard ordering and hence it only remains to prove the following assertion: let $\emptyset \neq M \subseteq A$ be a non-empty subset, then there is some $\mu \in M$ such that for any $\alpha \in M$ we get $\mu \leq_{\text{lex}} \alpha$. To do this we define

$$\begin{aligned}
\mu_1 &:= \min\{\, \alpha_1 \in \mathbb{N} \mid \alpha \in M \,\} \\
\mu_2 &:= \min\{\, \alpha_2 \in \mathbb{N} \mid \alpha \in M,\ \alpha_1 = \mu_1 \,\} \\
\ldots &\quad\ \ldots \\
\mu_n &:= \min\{\, \alpha_n \in \mathbb{N} \mid \alpha \in M,\ \alpha_1 = \mu_1, \ldots, \alpha_{n-1} = \mu_{n-1} \,\}
\end{aligned}$$

Hereby the set $\{\, \alpha_1 \mid \alpha \in M \,\}$ is non-empty, since $M \neq \emptyset$ was assumed to be non-empty. And $\{\, \alpha_2 \mid \alpha \in M, \alpha_1 = \mu_1 \,\}$ is non-empty, as there was some $\alpha \in M$ with $\alpha_1 = \mu_1$ and so forth. Hence μ is well defined and it is clear that $\mu \in M$, as $\mu = \alpha$ for some $\alpha \in M$. But the property $\mu \leq_{\text{lex}} \alpha$ is then clear from the construction.

- Now we will proof, that - assuming $(I, \leq)$ is a linearly ordered set - the ω-graded lexicographic order is a strictly positive partial order, as well. It is clear that $\leq_\omega$ inherits the property of being a partial order from $\leq_{\text{lex}}$ so it only remains to verify the strict positivity: Let $\alpha <_\omega \beta$, then we distinguish two cases. In the case $|\alpha|_\omega < |\beta|_\omega$ we clearly get

$$|\alpha + \gamma|_\omega \;=\; |\alpha|_\omega + |\gamma|_\omega \;<\; |\beta|_\omega + |\gamma|_\omega \;=\; |\beta + \gamma|_\omega$$

If on the other hand $|\alpha|_\omega = |\beta|_\omega$ then by assumption $\alpha <_{\text{lex}} \beta$ and as we have seen already this implies $\alpha + \gamma <_{\text{lex}} \beta + \gamma$. Thus in both cases we have found $\alpha + \gamma <_\omega \beta + \gamma$.

- We now assume that $(I, \leq)$ even is a well-ordered set and prove that $\leq_\omega$ is a total order in this case. Hence we need to regard the case that $\beta \leq_\omega \alpha$ is untrue. Of course this implies $|\alpha|_\omega \leq |\beta|_\omega$ and in the case $|\alpha|_\omega < |\beta|_\omega$ we are done already. Thus we may assume $|\alpha|_\omega = |\beta|_\omega$, but in this case the assumption reads as: $\neg\, \beta \leq_{\text{lex}} \alpha$. As we have seen above the lexicographic order is total and hence $\alpha <_{\text{lex}} \beta$ which conversely implies $\alpha <_\omega \beta$.

- In the final step we assume that I is finite, i.e. $I = 1 \ldots n$ and we need to show that $\leq_\omega$ is a well-ordering. Thus let $\emptyset \neq M \subseteq A$ be a non-empty subset again, then we have to verify that there is some $\mu \in M$ such that for any $\alpha \in M$ we get $\mu <_\omega \alpha$. To do this we define

$$\begin{aligned} m &:= \min\{\, |\alpha|_\omega \mid \alpha \in M \,\} \\ \mu &:= \min\{\, \alpha \mid \alpha \in M,\ |\alpha|_\omega = m \,\} \end{aligned}$$

 where the second minimum is taken under the lexicographic order. As M is non-empty m is well-defined and as $\leq_{\text{lex}}$ has been shown to be a well-ordering μ is well-defined, too. But $\mu \in M$ is trivial and $\mu \leq_\omega \alpha$ is clear from the construction.

□

15.9 Proofs of Chapter 8

Proof of (8.1):
In (i) we have to check that α truly is a homomorphism of rings. First of all we have $\varphi(1_R) = 1_R\,1_A = 1_A$ due to property (M.4) of the R-algebra A. Next we see $\varphi(a+b) = (a+b)1_A = (a\,1_A) + (b\,1_A) = \alpha(a) + \alpha(b)$ by property (M.2) of A. And lastly by properties (A) and (M.3) of A we also have

$$\begin{aligned}\varphi(a)\cdot\varphi(b) &= (a\,1_A)\cdot(b\,1_A) \;=\; a\,\big(1_A\dot{(}b\,1_A)\big)\\ &= a\,(b\,1_A) \;=\; (a\cdot b)\,1_A \;=\; \alpha(a\cdot b)\end{aligned}$$

Conversely for (ii) the properties (R) of an R-algebra are granted, as A has been assumed to be a ring. It remains to verify properties (M) and (A), as well. But these are straightforward, too:

$$\begin{aligned}a\,(s+t) &= \alpha(a)\cdot(s+t) \;=\; (\alpha(a)\cdot s) + (\alpha(a)\cdot t) \;=\; (a\,s) + (a\,t)\\ (a+b)\,s &= \alpha(a+b)\cdot s \;=\; \big(\alpha(a)+\alpha(b)\big)\cdot s\\ &= \big(\alpha(a)\cdot s\big) + \big(\alpha(b)\cdot s\big) \;=\; (a\,s) + (b\,s)\\ (a\cdot b)\,s &= \alpha(a\cdot b)\cdot s \;=\; \big(\alpha(a)\cdot\alpha(b)\big)\cdot s\\ &= \alpha(a)\cdot\big(\alpha(b)\cdot s\big) \;=\; a\,(b\,s)\\ 1_R\,s &= \alpha(1_R)\cdot s \;=\; 1_A\cdot s \;=\; s\\ (a\,s)\cdot t &= \big(\alpha(a)\cdot s\big)\cdot t \;=\; \alpha(a)\cdot\big(s\cdot t\big) \;=\; a\,(s\cdot t)\\ s\cdot(a\,t) &= s\cdot\big(\alpha(a)\cdot t\big) \;=\; \big(s\cdot\alpha(a)\big)\cdot t \;=\; \big(\alpha(a)\cdot s\big)\cdot t\\ &= \alpha(a)\cdot\big(s\cdot t\big) \;=\; a\,(s\cdot t)\end{aligned}$$

It remains to prove (iii): If S is R-torsion free we consider any a, $b \in R$ such that $a\,1_S = b\,1_S$. Then we have $(a-b)1_S = 0$, as $S \neq 0$ we have $1_S \neq 0_S$ and as S is torsion-free, this means $a = b$. But this already is the injectivity of α. Conversely if S is an integral domain and α is injective we consider any $a \in R$ and $s \in S$ such that $as = 0$. If $s = 0$ we are done, otherwise

$$0_R 1_S \;=\; 0_S \;=\; as \;=\; a(1_S\cdot s) \;=\; (a\,1_S)\cdot s$$

As $s \neq 0$ and S is an integral domain we conclude $a\,1_S = 0_S = 0_R 1_S$ and by the injectivity of α this is $a = 0$. That is we then find, that S truly is R-torsion-free. □

Proof of (8.2):

- Let us begin with (a) $\Longrightarrow$ (b): That is we need to show $as \in S$ for any $a \in R$ and any $s \in S$. Yet $S \;\leq_{\mathsf{r}}\; T$ is a sub-ring, in particular closed under multiplication and we have $as = a(1_T s) = (a1_T)s \in S$, as both $s \in S$ and $a1_T \in S$ by assumption (a).
- For (b) $\Longrightarrow$ (c) we note that $1_T \in S$ and S is closed under addition and multiplication, as $S \;\leq_{\mathsf{r}}\; T$ was assumed to be a sub-ring. And as we also have $as \in S$ for any $a \in R$ and $s \in S$, by assumption (b), we find $S \;\leq_{\mathsf{m}}\; T$. But a sub-module S with $1_T \in S$, that is closed under multiplication is a sub-algebra $S \;\leq_{\mathsf{a}}\; T$ of T.
- We have to close the circle, by proving (c) $\Longrightarrow$ (a): As $S \;\leq_{\mathsf{a}}\; T$ is a sub-algebra we have $1_T \in S$

and $as \in S$ for any $a \in R$ and $s \in S$. In particular $a1_T \in S$ for any $a \in R$, as S is closed under scalar-multiplication.

□

Proof of (8.4):

- We first want to show that for any $u_1, \ldots, u_n \in S$ the set $R[u_1, \ldots, u_n]$, defined explicitly as the set of all polynomial expressions $f(u_1, \ldots, u_n)$ where $f \in R[t_1, \ldots, t_n]$, is an R-algebra. To see this we note that in a ring extension $S : R$ both rings have been required to be commutative. Hence for any multi-indexes $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$ we find

$$u^{\alpha+\beta} \;=\; \prod_{k=1}^{n} u_k^{\alpha_k+\beta_k} \;=\; \prod_{k=1}^{n} u_k^{\alpha_k} \cdot u_k^{\beta_k} \;=\; \prod_{k=1}^{n} u_k^{\alpha_k} \cdot \prod_{k=1}^{n} u_k^{\beta_k} \;=\; u^{\alpha} \cdot u^{\beta}$$

 Thus the map $\sigma : \mathbb{N}^n \to S : \alpha \mapsto u^{\alpha}$ is a homomorphism of monoids. Also $\varphi : R \to S : a \mapsto a1_S$ is a homomorphism of rings, even of R-algebras. Therefore $\sigma_\varphi : R[t_1, \ldots, t_n] \to S : f \mapsto f(u_1, \ldots, u_n)$ is a homomorphism of rings, according to (7.14). But the property $\sigma_\varphi(af) = \varphi(a) \cdot \sigma_\varphi(f) = a1_S \cdot \sigma_\varphi(f) = a\sigma_\varphi(f)$ means that it even is a homomorphism of R-algebras.

 By construction we have $R[u_1, \ldots, u_n] = \mathrm{im}(\sigma_\varphi)$, such that this set is the image of an R-algebra homomorphism to S. In particular it is an R-algebra in itself - it is an R-module, according to (3.71) and a ring, according to (1.76).

- From here it is easy to see, that generally $R[U]$ is an R-algebra, as well. Given any two $x, y \in R[U]$ we find that $x \in R[u_1, \ldots, u_m]$ and $y \in R[v_1, \ldots, v_n]$ for some u_i and $v_j \in U$ respectively. But then both are contained in $R[u_1, \ldots, u_m, v_1, \ldots, v_n] \subseteq R[U]$. And hence the sum $x + y$ and product xy are contained in $R[u_1, \ldots, u_m, v_1, \ldots, v_n]$ and thereby in $R[U]$ again. Thus $R[U]$ is an R-algebra.

- As $R[U]$ is an R-algebra and clearly $U \subseteq R[U]$ we find the inclusion $\langle U \rangle_{\mathsf{a}} \subseteq R[U]$. Conversely consider any $Q \leq_{\mathsf{a}} S$ with $U \subseteq Q$. If now $x = f(u_1, \ldots, u_n) \in R[U]$ then any $u_k \in U \subseteq Q$ and hence $x \in Q$. Thus we have $R[U] \subseteq Q$ and as this is true for any such Q we also find $R[U] \subseteq \langle U \rangle_{\mathsf{a}}$.

□

Proof of (8.5):
If $S : R$ is a ring-extension and $u_1, \ldots, u_k \in S$ are elements of S, then by construction of polynomials $f \in R[t_1, \ldots, t_k]$ and the evaluation of f on the u_i, the elements of $R[u_1, \ldots, u_k]$ are of the form

$$f(u_1, \ldots, u_k) \;=\; \sum_{\alpha \in \mathbb{N}^k} f[\alpha]\, u_1^{\alpha_1} \ldots u_k^{\alpha_k}$$

Let us abbreviate the intermediate ring $A := R[u_1, \ldots, u_k]$ of $S : R$ for the time being. Then consequentially, if $u_{k+1}, \ldots, u_n \in S$ are another elements of S (not necessarily distinct from $u_1, \ldots, u_k$) then an element of $A[u_{k+1}, \ldots, u_n]$ is of the form

$$g(u_{k+1}, \ldots, u_n) \;=\; \sum_{\beta \in \mathbb{N}^{n-k}} g[\beta]\, u_{k+1}^{\beta_{k+1}} \ldots u_n^{\beta_n}$$

where $g[\beta] \in A = R[u_1, \ldots, u_k]$. That is every $g[\beta]$ is of the form above and inserting this into $g(u_{k+1}, \ldots, u_n)$ we find an element of S, of the form

$$\sum_{\beta \in \mathbb{N}^{n-k}} \sum_{\alpha \in \mathbb{N}^k} g[\beta][\alpha]\, u_1^{\alpha_1} \ldots u_k^{\alpha_k} u_{k+1}^{\beta_{k+1}} \ldots u_n^{\beta_n}$$

Letting $\gamma := (\alpha, \beta) \in \mathbb{N}^n$ we see, that this $g(u_{k+1}, \ldots, u_n)$ is an element of $R[u_1, \ldots, u_n]$, as it is of the form

$$g(u_{k+1}, \ldots, u_n) \;=\; \sum_{\gamma \in \mathbb{N}^n} g[\beta][\alpha]\, u_1^{\gamma_1} \ldots u_n^{\gamma_n}$$

So this is any $g(u_{k+1}, \ldots, u_n) \in R[u_1, \ldots, u_k][u_{k+1}, \ldots, u_n]$ also is an element of $R[u_k, \ldots, u_n]$ and hence the respective inclusion. Conversely it is clear, that any element of $h(u_1, \ldots, u_n) \in R[u_1, \ldots, u_n]$ can be rearranged in such a way, that we see that it also is an element of $R[u_1, \ldots, u_k][u_{k+1}, \ldots, u_n]$, as it can be written in the form

$$\sum_{\beta \in \mathbb{N}^{n-k}} \left(\sum_{\alpha \in \mathbb{N}^k} h[\alpha, \beta]\, u_1^{\alpha_1} \ldots u_k^{\alpha_k} \right) u_{k+1}^{\beta_{k+1}} \ldots u_n^{\beta_n}$$

That is we have see the following identity of intermediate rings of $S : R$ given arbitrary, but finitely many, elements $u_1, \ldots, u_n$ of S

$$R[u_1, \ldots, u_k][u_{k+1}, \ldots, u_n] \;=\; R[u_1, \ldots, u_n]$$

In other words, we have $R[U][V] = R[U \cup V]$ for any finite subsets U, $V \subseteq S$. However, if U, $V \subseteq S$ are arbitrary subsets of S, then any element $h \in R[U \cup V]$ is contained in some $R[U_0 \cup V_0]$ for some *finite* subsets $U_0 \subseteq U$ and $V_0 \subseteq V$. Thus we have seen $h \in R[U_0][V_0] \subseteq R[U][V]$ and hence $R[U \cup V] \subseteq R[U][V]$. Conversely if $g \in R[U][V]$ then $g \in R[U][V_0]$ for some finite subset $V_0 = \{ v_1, \ldots, v_n \} \subseteq V$. That is g is of the form

$$g \;=\; \sum_{\beta \in \mathbb{N}^n} g[\beta]\, v_1^{\beta_1} \ldots u_n^{\beta_n}$$

where only finitely many $g[\beta] \in R[U]$ are non-zero. For any such $g[\beta]$ there is a finite subset $U_\beta \subseteq U$ such that $g[\beta] \in R[U_\beta]$ (if $g[\beta] = 0$ we can take $U_\beta = \emptyset$). Now let

$$U_0 \;:=\; \bigcup_{\beta \in \mathbb{N}^n} U_\beta \;\subseteq\; U$$

By construction this is a finite subset of U and we have $g \in R[U_0][V_0]$ which is $g \in R[U_0 \cup V_0] \subseteq R[U \cup V]$ as we have seen above. That is we also have $R[U][V] \subseteq R[U \cup V]$ and hence the equality of these intermediate rings. □

Proof of (8.6):

- For (a) $\implies$ (b) it suffices to note that $S \leq_{\mathsf{a}} T$ is a sub-algebra of T, by assumption. Thus if also $U \subseteq S$, then the sub-algebra generated by U is contained in S, as well: $\langle U \rangle_{\mathsf{a}} \subseteq S$. But this is $R[U] = \langle U \rangle_{\mathsf{a}}$, already. The implication (b) $\implies$ (c) is trivial by taking $U := \{ u, v \}$.
- Finally for (c) $\implies$ (a): As 0_T and $1_T \in R[u, v]$ we also have 0_T and $1_T \in S$. Now consider any u, $v \in S$ and $a \in R$, then au, $u + v$ and $uv \in R[u, v] \subseteq S$. That is S is closed under scalar-multiplication, addition and multiplication, which means $S \leq_{\mathsf{a}} T$ is a sub-algebra and hence an

intermediate ring.

□

Proof of (8.7):

(i) Consider any $z \in T$, as Y generates T as an S-module there are some $y_1, \ldots, y_n \in Y$ and some $s_1, \ldots, s_n \in S$ such that

$$z = \sum_{j=1}^{n} s_j y_j$$

But S is generated by X, as an R-module, that is for any $j \in 1 \ldots n$ there are some $x_{1,j}, \ldots, x_{m(j),j} \in X$ and $a_{1,j}, \ldots, a_{m(j),j} \in R$ such that

$$s_j = \sum_{i=1}^{m(j)} a_{i,j} x_{i,j}$$

Combining these equations we find that z is an R-linear combination of elements of the form $x_{i,j} y_j \in XY$ and hence T is generated by XY, as an R-module

$$z = \sum_{j=1}^{n} \sum_{i=1}^{m(j)} a_{i,j} x_{i,j} y_j$$

(ii) Consider some $a_1, \ldots, a_n \in R$ and some pairwise distinct $z_1, \ldots, z_n \in XY$ (that is $z_k = x_k y_k$ for some $x_k \in X$ and $y_k \in Y$) such that

$$\sum_{k=1}^{n} a_k z_k = 0$$

Renumbering we may assume w.l.o.g. that $y_1, \ldots, y_m$ is a collection of distinct elements of $\{ y_1, \ldots, y_n \}$ and for any $i \in 1 \ldots m$ we denote $K_i := \{ k \in 1 \ldots n \mid y_k = y_i \}$. That is $\{ K_1, \ldots, K_m \}$ is a partition of $1 \ldots n$. Then we find that

$$0 = \sum_{k=1}^{n} a_k z_k = \sum_{i=1}^{m} \left(\sum_{k \in K_i} a_k x_k \right) y_i$$

As Y is S-linearly independent and the y_i are pairwise distinct we conclude that for any $i \in 1 \ldots m$ we necessarily have

$$0 = \sum_{k \in K_i} a_k x_k$$

For any $i \in 1 \ldots m$ and any two indices $p \neq q \in K_i$ the elements x_p and x_q are distinct $x_p \neq x_q$, as else $z_p = x_p y_i = x_q y_i = z_q$ in contradiction to the pairwise distinctness of the z_k. Yet as X is R-linearly independent we conclude that for any $k \in K_i$ we must have $a_k = 0$. And as any $k \in 1 \ldots n$ is contained in one of the K_i we have $a_k = 0$ for any $k \in 1 \ldots n$.

(iii) A basis is a linearly independent set, that generated a s a module. Thus this statement is an immediate consequence of (i) and (ii) combined.

(iv) Let $X \subseteq S$ be a set of generators of S as an R-module, of minimal cardinality, that is $|X| = [S : R]$. Likewise pick up $Y \{ T \}$ such that $|Y| = [T : S]$. By (i) we know that XY generates T as an R-module and hence $[T : R] \leq |XY|$. But clearly $X \times Y \twoheadrightarrow XY : (x, y) \mapsto xy$ is a surjective map

and hence $|XY| \leq |X \times Y| = |X| \cdot |Y|$. Thus we have the chain of inequalities

$$[T:R] \;\leq\; |XY| \;\leq\; |X \times Y| \;=\; |X| \cdot |Y| \;=\; [S:R] \cdot [T:S]$$

Which proves the first part. If now R and S are fields, then we may even choose an R-basis $X \subseteq S$ of S and an S-basis $Y \subseteq T$ of T. By (iii) XY then is an R-basis of T and hence we have $[T:R] = |XY|$. Yet, as XY is R-linearly independent the elements $xy \in XY$ also have to be pairwise distinct. That is the map $X \times Y \longleftrightarrow XY : (x,y) \mapsto xy$ is bijective, in this case. And therefore all the above inequalities turn into equalities

$$[T:R] \;=\; |XY| \;=\; |X \times Y| \;=\; |X| \cdot |Y| \;=\; [S:R] \cdot [T:S]$$

□

Proof of (8.10):

(i) Let us denote $x := t + fR[t]$ and $\mathcal{M} := \{\, x^k \mid 0 \leq k < n \,\}$. We will first prove that $\mathcal{M}$ is a generating set of S as an R-module: If $g \in R[t]$ is any polynomial, then we may use division with remainder (as f is monic) to find some $q, r \in R[t]$ such that

$$g \;=\; qf + r$$

and $r = 0$ or $\deg(r) < n$. Thereby $g + fR[t] = qf + r + fR[t] = r + fR[t]$ and as $\deg(r) < n$ this means $g + fR[t] = r[0]x^0 + r[1]x^1 + \cdots + r[n-1]x^{n-1}$ such that $g + fR[t]$ can be generated as an R-linear combination over $\mathcal{M}$. As g has been arbitrary this is

$$S \;=\; \mathrm{Lh}\{\, x^0, x^1, \ldots, x^{n-1} \,\} \;=\; \Big\{\, t^k + fR[t] \mid 0 \leq k < n \,\Big\}$$

To complete that $\mathcal{M}$ is an R-basis of S, as an R-module, we have to prove the linear independence of $\mathcal{M}$: Suppose there were some $a_0, a_1, \ldots, a_{n-1} \in R$ satisfying a relation of the form

$$\sum_{k=0}^{n-1} a_k x^k \;=\; \sum_{k=0}^{n-1} a_k t^k + fR[t] \;=\; 0 + fR[t]$$

That is $r(t) := a_0 t^0 + a_1 t^1 + \cdots + a_{n-1} t^{n-1} \in fR[t]$ such that $r = fg$ for some polynomial $g \in R[t]$. Suppose we had $g \neq 0$, as f is monic the leading coefficients of g and f cannot cancel each other, such that $\deg(r) = \deg(fg) = \deg(f) + \deg(g) \geq \deg(f) = n$ - refer to (7.18) for more details on this. However $\deg(r) \leq n - 1 < n$. This contradiction yields $g = 0$ and hence $r = 0$. But this again is $a_k = 0$ for any $k \in 0 \ldots (n-1)$ and hence $\mathcal{M}$ is linearly independent.

In particular: As $n \geq 1$ we find that $\{\, x \,\}$ is R-linearly independent. Hence suppose $\alpha(a) = \alpha(b)$ for some $a, b \in R$. Then $ax = bx$ such that $(a-b)x = 0 + fR[t]$. As we have seen above, this implies $a - b = 0$ and hence $a = b$, such that α is injective.

(ii) As $\deg(f) \geq 1$ there is some $k \in \mathbb{N}$ such that $f[k] \neq 0$. In particular $R \neq 0$ is not the zero-ring. Let us now use induction on n: In case $n = 1$, as f is monic, it is of the form $f(t) = t + f[0]$. That is we may take $S = R$ and $s_1 := -f[0]$ and are already done.

For the induction step we consider $\deg(f) = n$ and may assume the claim for any polynomial $q \in R[t]$ of degree $\deg(q) < n$. So we start out with

$$S_1 \;:=\; R[t_1] \Big/ f(t_1)R[t_1]$$

Again we abbreviate $x := t_1 + f(t_1)R[t_1]$ then we have seen in (i), that $S_1 : R$ is a ring extension under $\alpha : R \hookrightarrow S : a \mapsto ax^0$ and that $[S_1 : R] = n$. Also, as $g \mapsto g + f(t_1)R[t_1]$ is a homomorphism of R-algebras, we find that

$$f(x) \;=\; f\Big(t_1 + f(t_1)R[t_1]\Big) \;=\; f(t_1) + f(t_1)R[t_1] \;=\; 0 + f(t_1)R[t_1]$$

That is $f(x) = 0 \in S_1$ and hence $(t - x)$ divides f in $S_1[t]$, according to (7.54.(iii)). That is there is some $q \in S_1[t]$ such that $f(t) = q(t)(t - x)$. And as f is monic, (7.54.(i)) tells us, that q thereby is a monic polynomial of degree $n - 1$. Hence we may use the induction hypothesis on q to find another ring extension $S : S_1$ under $\beta : S_1 \hookrightarrow S$ such that $[S : S_1] \leq (n-1)!$ and q splits over S. That is

$$q(t) \;=\; (t - s_2) \dots (t - s_n)$$

for some sufficient $s_k \in S$. Let $s_1 := \beta(x) \in S$. By definition of the scalar multiplication of S we have $xq = \beta(x) \cdot q = s_1 q$ such that $f = (t - x)q = tq - xq = tq - s_1 q = (t - s_1)q$. Replacing q with its factorisation again, we have proved property (3)

$$f(t) \;=\; (t - s_1)(t - s_2) \dots (t - s_n)$$

Also property (1) is a given: Just take $S : R$ under the monomorphism $\beta\alpha : R \hookrightarrow S$. We have $[S_1 : R] = n$ by (i) and $[S : S_1] \leq (n-1)!$ by induction hypothesis. Now use the degree-formula (8.7.(iv)) to also find property (2)

$$[S : R] \;\leq\; [S : S_1] \cdot [S_1 : R] \;\leq\; (n-1)! \cdot n \;=\; n$$

(iii) Obviously we use induction on the number r of polynomials given. The case $r = 1$ has already been dealt with in (ii) so we continue with the induction step right away: By (ii) there is a ring extension $\alpha : R \to S_1$ such that f_1 splits over S_1. That is there are elements $x_j \in S$ such that

$$f_1(t) \;=\; \prod_{j=1}^{n(1)} (t - x_j)$$

Note that $[S_1 : R] \leq n_1! < \infty$ is finite. And as we have to compare these polynomials in $S_1[t]$, on a formal, set-theoretic basis, this identity reads as

$$\alpha(f_1)(t) \;=\; \prod_{j=1}^{n(1)} (t - x_j)$$

Let us now consider $\alpha(f_i) \in S_1[t]$ in the sense of (7.12.(iv)) for any $i \in 2 \dots r$. Now, by induction hypothesis, there is another ring extension $\beta : S_1 \hookrightarrow S$ such that all the $\alpha(f_i)$ split simultaneously.

That is there are elements $s_{i,j} \in S$ (where $i \in 2 \dots r$ and $j \in 1 \dots n(i)$) such that

$$\alpha(f_i)(t) \;=\; \prod_{j=1}^{n(i)} (t - s_{i,j})$$

By definition these identities compare the coefficients $\beta\alpha(f_i[k])$ of the left-hand side, with the coefficients of the right-hand side. But if we consider $f_i \in R[t]$ and the ring extension $S : R$ under $\beta\alpha : R \hookrightarrow S$, then the same is true for the identities

$$f_i(t) \;=\; \prod_{j=1}^{n(i)} (t - s_{i,j})$$

That is the $f_i \in R[t]$ for $i \in 2 \dots r$ split over S. Let us denote $s_{1,j} := \beta(x_j) \in S$, as f_1 splits over S_1 and $S : S_1$ is an extension of S_1 (8.9) tells us, that f_1 also splits over S in the just the same form

$$f_1(t) \;=\; \prod_{j=1}^{n(1)} (t - s_{1,j})$$

Thus if we take $\beta\alpha : R \hookrightarrow S$ as a ring extension, properties (1) and (3) are already satisfied. Now recall that by induction hypothesis we have $[S : S_1] < \infty$, as well. Thus the degree formula (8.7.(iv)) grants property (2) again, as we get

$$[S : R] \;\leq\; [S : S_1] \cdot [S_1 : R] \;<\; \infty$$

(iv) Let us first consider the case of a monic polynomial $f \in E[t]$, where E is a field. In this case $E[t]$ is an euclidean domain and hence an UFD such that we can modify the construction in (i) a little: We can choose a monic prime factor p of f, that is p is irreducible and $f = pg$ for some $g \in E[t]$. Then we have $1 \leq \deg(p) \leq \deg(f)$ and let $F := E[t]/pE[t]$. By (i) above $\alpha : E \hookrightarrow F$ is a finite ring of degree $[F : E] = \deg(p)$. And for $x := t + pE[t]$ we get $f(x) = p(x)g(x) = pg + pE[t] = 0$ again. As $pE[t]$ is a prime ideal and $p \neq 0$ we know by (2.79.(i)) that $pE[t]$ is a maximal ideal and hence $F = E[t]/pE[t]$ is a field. Thus we find a field F, such that $[F : E] \leq \deg(f)$ is finite and $f(x) = 0$ for some $x \in F$.

As in (ii) this process can be used inductively: Pick up a monic prime factor p_1 of f. Then by the above $F_1 := E[t_1]/p_1(t_1)E[t_1]$ is a field, $F_1 : E$ is a field extension of degree $[F_1 : E] \leq \deg(f)$ and $f = p_1 q_1$. Consider $q_1 \in F_1[t]$, then by induction hypothesis there is a field extension $[F : F_1]$ such that q_1 splits in F and $[F : F_1] \leq \deg(q_1)$. Then f splits over F, as in (ii).

Now for a general polynomial $f \in E[t]$ of $n = \deg(f) \geq 1$, where E is a field. In this case we let $a := \mathrm{lc}(f) \in E$. As $a \neq 0$ we have $a \in E^*$ and thereby $m := a^{-1}f$ is a monic polynomial of degree $\deg(m) = \deg(f)$. For this we have just seen, that there is a field F, such that $E \hookrightarrow F$ is a ring extension with $[F : E] \leq \deg(m)! = \deg(f)!$ and m splits over F. That is there are some $x_1, \dots, x_n \in F$ such that m and with it f can be written in the following form

$$f(t) \;=\; am(t) \;=\; a\prod_{i=1}^{n}(t - x_i)$$

□

Proof of (8.14):
As $A \subseteq \mathfrak{a}$ we have $\alpha(A) \subseteq \alpha(\mathfrak{a}) \subseteq \mathfrak{a}S$ such that $\langle \alpha(A) \rangle_{\mathfrak{i}} \subseteq \mathfrak{a}S$ is clear. For the converse inclusion we start with some $f \in \mathfrak{a}S$, that is there are some $s_k \in S$ and $b_k \in \mathfrak{a}$ such that

$$f \;=\; s_1 \cdot \alpha(b_1) + \cdots + s_n \cdot \alpha(b_n)$$

But as $\mathfrak{a}$ is generated by A, for any $k \in 1 \ldots n$ there are some $r_{i,k} \in R$ and $a_{i,k} \in A$ such that all the b_k are of the form

$$b_k \;=\; \sum_{i=1}^{m(k)} r_{i,k} a_{i,k}$$

Combining these equations we find that $f \in \langle \alpha(A) \rangle_{\mathfrak{i}}$, as well, since any $\alpha(a_{i,k}) \in \alpha(A)$ such that f is just an S-linear combination of elements of $\alpha(A)$:

$$f \;=\; \sum_{k=1}^{n} s_k \alpha(b_k) \;=\; \sum_{k=1}^{n} s_k \sum_{i=1}^{m(k)} \alpha(r_{i,k}) \alpha(a_{i,k}) \;=\; \sum_{k=1}^{n} \sum_{i=1}^{m(k)} s_k \alpha(r_{i,k}) \alpha(a_{i,k})$$

□

Proof of (8.15):
Given the structural homomorphism $\alpha : R \to S$ and an ideal $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$ we have defined the ideal $\mathfrak{a}S$ to be $\mathfrak{a}\,S = \langle \alpha(a) \mid a \in \mathfrak{a} \rangle_{\mathfrak{i}}$. In particular we have $\alpha(\mathfrak{a}) \subseteq \mathfrak{a}S$ and therefore $\mathfrak{a} \subseteq \mathfrak{b}$ implies $\alpha(\mathfrak{a}) \subseteq \alpha(\mathfrak{b}) \subseteq \mathfrak{b}\,S$, such that $\mathfrak{a}\,S \subseteq \mathfrak{b}\,S$ again. And for an ideal $\mathfrak{u} \trianglelefteq_{\mathfrak{i}} S$ we have defined $\mathfrak{u} \cap R = \alpha^{-1}(\mathfrak{u})$. In particular $\mathfrak{u} \subseteq \mathfrak{v}$ implies $\mathfrak{u} \cap R = \alpha^{-1}(\mathfrak{u}) = \alpha^{-1}(\mathfrak{v}) = \mathfrak{v} \cap R$. Now (0.7) yields

$$\mathfrak{a} \;\subseteq\; \alpha^{-1}\big(\alpha(\mathfrak{a})\big) \;\subseteq\; \alpha^{-1}\big(\mathfrak{a}\,S\big) \;=\; \big(\mathfrak{a}\,S\big) \cap R$$

And if $\mathfrak{u} \trianglelefteq_{\mathfrak{i}} S$ is an ideal in S then by definition any $x \in (\mathfrak{u} \cap R)S$ is of the form $x = s_1\alpha(a_1) + \cdots + s_n\alpha(a_n)$ where $s_k \in S$ and $a_k \in \mathfrak{u} \cap R$. But the latter is $\alpha(a_k) \in \mathfrak{u}$ and as $\mathfrak{u}$ is an ideal this means $x \in \mathfrak{u}$ again. As x has been arbitrary, this is the inclusion we aimed for

$$\big(\mathfrak{u} \cap R\big)\,S \;\subseteq\; \mathfrak{u}$$

Altogether we have proved property (b) of a covariant Galois-connection. Now by (0.24) this implies the identities for ideals of the form $\mathfrak{a}\,S \trianglelefteq_{\mathfrak{i}} S$ and $\mathfrak{u} \cap R \trianglelefteq_{\mathfrak{i}} R$ respectively. Also we find the 1-to-1 correspondence between ideals of this kind. In particular we have $(\mathfrak{a}\,S) \cap R = \mathfrak{a}$ for any $\mathfrak{a} = \mathfrak{u} \cap R$. And this already is the implication (b) $\implies$ (a) for prime ideals. In the converse direction (a) $\implies$ (b) we have $\mathfrak{p} = (\mathfrak{p}\,S) \cap R$ and need to find some $\mathfrak{q}$ such that $\mathfrak{p} = \mathfrak{q} \cap R$. To find this note that $U := R \setminus \mathfrak{p}$ is multiplicatively closed and hence $\alpha(U) \subseteq S$ is multiplicatively closed, too. We now argue, that

$$\alpha(U) \cap \mathfrak{p}\,S \;=\; \emptyset$$

Suppose there was some $a \in U$ with $\alpha(a) \in \mathfrak{p}\,S$, then this would mean $a \in \alpha^{-1}(\mathfrak{p}\,S) = (\mathfrak{p}\,S) \cap R = \mathfrak{p}$. But by construction of U this is absurd. We now denote $S_{\mathfrak{p}} := \alpha(U)^{-1}S$ and let $\mathfrak{u} := (\mathfrak{p}\,S)\,S_{\mathfrak{p}} \trianglelefteq_{\mathfrak{i}} S_{\mathfrak{p}}$ be the ideal $\mathfrak{p}\,S$ pushed further to $S_{\mathfrak{p}}$. Suppose we had $\mathfrak{u} = S_{\mathfrak{p}}$, then $1 \in \mathfrak{u}$, where 1 in $S_{\mathfrak{p}}$ is $1_S/1_S$. By

construction of $\mathfrak{u}$ this would mean that there would be some $s_1,\ldots,s_n \in S$, $u_1,\ldots,u_n \in U$ and some $q_1,\ldots,q_n \in \mathfrak{p}S$ such that

$$\frac{1_S}{1_S} \;=\; \frac{s_1}{\alpha(u_1)}\cdot\frac{q_1}{1_S}+\cdots+\frac{s_n}{\alpha(u_n)}\cdot\frac{q_n}{1_S} \;=\; \frac{t_1q_1+\cdots+t_nq_n}{\alpha(u_1)\ldots\alpha(u_n)}$$

where $t_1 := s_1\alpha(u_2)\cdot\cdots\cdot\alpha(u_n)$ and so on, until $t_n := s_n\alpha(u_1)\cdot\cdots\cdot\alpha(u_{n-1})$. As $\mathfrak{p}S \trianglelefteq_{\mathrm{i}} S$ is an ideal $q := t_1q_1+\cdots+t_nq_n \in \mathfrak{p}S$ and using $u := u_1\cdot\cdots\cdot u_n$ the equation above turns into $\alpha(v)\alpha(u) = \alpha(v)q \in \mathfrak{p}S$ for some $v \in U$. But $\alpha(uv) \in \mathfrak{p}S$ cannot be, as $\alpha(U)\cap\mathfrak{p}S = \emptyset$ and hence we get

$$\mathfrak{u} \;:=\; (\mathfrak{p}\,S)\,S_{\mathfrak{p}} \;\neq\; S_{\mathfrak{p}}$$

And thereby there is a maximal ideal $\mathfrak{n} \trianglelefteq_{\mathrm{i}} S_{\mathfrak{p}}$ that contains $\mathfrak{u} \subseteq \mathfrak{n}$. And for this ideal we then find the following chain of inclusions

$$\mathfrak{p}\,S \;\subseteq\; (\mathfrak{p}\,S_{\mathfrak{p}})\cap S \;\subseteq\; \mathfrak{u}\cap S \;\subseteq\; \mathfrak{n}\cap S$$

In the end we have $\mathfrak{p}\,S \subseteq \mathfrak{n}\cap S$. Let us denote $\mathfrak{q} := \mathfrak{n}\cap S$. We will see that this is the proper candidate for (a). To do this, as a next step, we claim

$$\mathfrak{q}\cap\alpha(U) \;=\; \emptyset$$

Suppose there was some $a \in U$ with $\alpha(a) \in \mathfrak{q}$. This would mean $\alpha(a)/1_S \in \mathfrak{n}$ and as $\mathfrak{a}(a)/1_S$ is a unit in $S_{\mathfrak{p}}$ this would imply $\mathfrak{n} = S_{\mathfrak{p}}$. But as $\mathfrak{n}$ is a maximal ideal this is not the case. We can now use the assumption on $\mathfrak{p}$ and the inclusion $\mathfrak{p}\,S \subseteq \mathfrak{q}$ to find another inclusion

$$\mathfrak{p} \;=\; (\mathfrak{p}\,S)\cap R \;\subseteq\; \mathfrak{q}\cap R$$

But as $\mathfrak{q}\cap\alpha(U) = \emptyset$ we also have $\emptyset = \alpha^{-1}(\mathfrak{q})\cap\alpha^{-1}(\alpha(U)) \supseteq (\mathfrak{q}\cap R)\cap U$. This can be reformulated, as $\mathfrak{q} \subseteq R\setminus U = \mathfrak{p}$ (by construction of U). Thus we also have the converse inclusion

$$\mathfrak{q}\cap R \;\subseteq\; \mathfrak{p}$$

Together $\mathfrak{p} \subseteq \mathfrak{q}\cap R$ and $\mathfrak{q}\cap R \subseteq \mathfrak{p}$ yield property (a) $\mathfrak{p} = \mathfrak{q}\cap R$ which had to be derived from (b). □

Proof of (8.17):

(i) By definition of the scalar multiplication in $S : R$ we have $as = \iota(a)\cdot s$. And as π is a homomorphism of rings, this turns into

$$\pi\big(as\big) \;=\; \pi\big(\iota(a)\cdot s\big) \;=\; \pi\iota(a)\cdot\pi(s) \;=\; a\cdot\pi(s)$$

(ii) By definition $\pi^{-1}(\mathfrak{a}) = \{\, s\in S \mid \pi(s)\in\mathfrak{a}\,\}$ and the ideal $\mathfrak{a}S$ is generated by $\iota(\mathfrak{a}) = \{\,\iota(a)\mid a\in\mathfrak{a}\,\}$. Thus if we start with $s = \iota(a) \in \iota(\mathfrak{a})$, then we have $\pi(s) = \pi\iota(a) = a \in \mathfrak{a}$, such that $s \in \pi^{-1}(\mathfrak{a})$. Hence we have $\iota(\mathfrak{a}) \subseteq \pi^{-1}(\mathfrak{a})$, but as the letter is an ideal, the same is true for the ideal generated by this set $\mathfrak{a}S \subseteq \pi^{-1}(\mathfrak{a})$.

(iii) This is trivial, if we just look at the definition $\mathfrak{u}\cap R = \iota^{-1}(\mathfrak{u}) = \{\, a\in R \mid \iota(a)\in\mathfrak{u}\,\}$. If we start

with some $a \in R$ such that $\iota(a) \in \mathfrak{u}$, then $a = \pi\iota(a) \in \pi(\mathfrak{u})$ such that $\mathfrak{u} \cap R \subseteq \pi(\mathfrak{u})$.

□

Proof of (8.18):
By definition of the pull-back we have $(\mathfrak{c} \cap S) \cap R = \alpha^{-1}(\mathfrak{c} \cap S) = \alpha^{-1}(\beta^{-1}(\mathfrak{c})) = (\beta\alpha)^{-1}(\mathfrak{c}) = \mathfrak{c} \cap R$. Thus the second identity is done already. For the first let us begin with the inclusion $\mathfrak{a}T \subseteq (\mathfrak{a}S)T$: Given any $g \in \mathfrak{a}T$ there are some $t_1, \ldots, t_n \in T$ and $a_1, \ldots, a_n \in \mathfrak{a}$ such that $g = t_1\beta\alpha(a_1) + \cdots + t_n\beta\alpha(a_n)$. With $f_i := \alpha(a_i) \in \mathfrak{a}S$ this means $g = t_1\beta(f_1) + \cdots + t_n\beta(f_n)$ and hence $g \in (\mathfrak{a}S)T$.
Now for $(\mathfrak{a}S)T \subseteq \mathfrak{a}T$ we start with some g of the form $g = t_1\beta(f_1) + \cdots + t_n\beta(f_n)$, where $t_k \in T$ and $f_k \in \mathfrak{a}S$. That is the f_k are of the form $f_k = s_{1,k}\alpha(a_{1,k}) + \cdots + s_{m(k),k}\alpha(a_{m(k),k})$ where $s_{i,k} \in S$ and $a_{i,k} \in \mathfrak{a}$. Combining these we find $g \in \mathfrak{a}T$, as

$$g \;=\; \sum_{k=1}^{n} t_k\beta(f_k) \;=\; \sum_{k=1}^{n}\sum_{i=1}^{m(k)} t_k\beta(s_{i,k}) \cdot \beta\alpha(a_{i,k}) \;\in\; \mathfrak{a}T$$

□

Proof of (8.19):

(i) We prove the well-definedness and injectivity of $a + \mathfrak{a} \mapsto \alpha(a) + \mathfrak{u}$ at the same time: Consider any $a, b \in R$ with $a + \mathfrak{a} = b + \mathfrak{a}$, this is equivalent, to $b - a \in \mathfrak{a} = \mathfrak{u} \cap R = \alpha^{-1}(\mathfrak{u})$. And this is just a reformulation of $\alpha(b - a) \in \mathfrak{u}$. Now, as α is a homomorphism this again is equivalent, to $\alpha(a) + \mathfrak{u} = \alpha(b) + \mathfrak{u}$ so altogether we have

$$a + \mathfrak{a} \;= b + \mathfrak{a} \quad\Longleftrightarrow\quad \alpha(a) + \mathfrak{u} \;= \alpha(b) + \mathfrak{u}$$

In this equivalence $\Longrightarrow$ is the well-definedness and $\Longleftarrow$ is the injectivity of the map. So we are done in case of $\mathfrak{a} = \mathfrak{u} \cap R$.

(ii) Again consider $a, b \in R$ such that $a + \mathfrak{a} = b + \mathfrak{a}$. Again this is $b - a \in \mathfrak{a}$ and hence $\alpha(b - a) \in \alpha(\mathfrak{a}) \subseteq \mathfrak{a}S = \mathfrak{u}$. Thus we have $\alpha(a) + \mathfrak{u} = \alpha(b) + \mathfrak{u}$ which means $a + \mathfrak{a} \mapsto \alpha(a) + \mathfrak{u}$ is well-defined. Now suppose $\mathfrak{a} = (\mathfrak{a}S) \cap R = \mathfrak{u} \cap R$ then we also need to show the injectivity: If $\alpha(a) + \mathfrak{u} = \alpha(b) + \mathfrak{u}$ then we get $b - a \in \mathfrak{u} \cap R$ as in (i) before. Thus we have $b - a \in \mathfrak{a}$ by assumption on $\mathfrak{a}$ and hence $a + \mathfrak{a} = b + \mathfrak{a}$ which is the injectivity.

□

Proof of (8.21):
As usual let $\alpha : R \to S$ be the structural homomorphism of $S : R$, that is $\alpha(a) = a \cdot 1_S$. Then we will first prove the identity and inclusion for the pull-back and then the identity and inclusion for the push-out - in this order. Let us commence:

(i) Consider any $a \in R$ then we will prove that a is contained in the intersection of the $\mathfrak{u}_\lambda \cap R$ if and only if a is contained in the pull-back of the intersection of the $\mathfrak{u}_\lambda$. This will be the first identity:

$$\begin{aligned} a \in \bigcap_{\lambda\in\Lambda} (\mathfrak{u}_\lambda \cap R) \quad &\Longleftrightarrow \quad \forall\, \lambda \in \Lambda \,:\, a \in \mathfrak{u}_\lambda \cap R \\ &\Longleftrightarrow \quad \forall\, \lambda \in \Lambda \,:\, \alpha(a) \in \mathfrak{u}_\lambda \end{aligned}$$

$$\begin{aligned} &\iff \quad \alpha(a) \in \bigcap_{\lambda\in\Lambda} \mathfrak{u}_\lambda \\ &\iff \quad a \in \left(\bigcap_{\lambda\in\Lambda} \mathfrak{u}_\lambda\right) \cap R \end{aligned}$$

(i) Let $\mathfrak{u}$ be the sum of all the $\mathfrak{u}_\lambda$ and consider some a contained in the sum of the pull-backs $\mathfrak{u}_\lambda \cap R$. The sum is generated by the union of the $\mathfrak{u}_\lambda \cap R$ and hence a is of the form

$$a \;=\; b_1 a_1 + \cdots + b_r a_r$$

for some $b_i \in R$ and $a_i \in \mathfrak{u}_{\lambda(i)} \cap R$ for some $\lambda(i) \in \Lambda$. That is $\alpha(a_i) \in \mathfrak{u}_{\lambda(i)}$ and hence we insert a into α. If we denote $s_i := \alpha(b_i) \in S$ then we find (as α is a homomorphism of rings)

$$\alpha(a) \;=\; s_1\,\alpha(a_1) + \cdots + s_r\,\alpha(a_r)$$

As any $\alpha(a_i) \in \mathfrak{u}_{\lambda(i)} \subseteq \mathfrak{u}$ we see, that $\alpha(a)$ is contained in $\mathfrak{u}$ again. And by definition this means $a \in \mathfrak{u} \cap R$, which had to be shown.

(i) By definition of the product of ideals, the elements $c \in (\mathfrak{u} \cap R) \cdot (\mathfrak{v} \cap R)$ are of the following form (for some a_k, $b_k \in R$, such that $\alpha(a_k) \in \mathfrak{u}$ and $b_k \in \mathfrak{b}$)

$$c \;=\; \sum_{k=1}^{n} a_k b_k$$

Therefore find $\alpha(a_k)\alpha(b_k) \in \mathfrak{u} \cdot \mathfrak{v}$, so if we apply α to c and use its homomorphism properties, we find that $\alpha(c) \in \mathfrak{u} \cdot \mathfrak{v}$, as well (see below). But this just is $c \in (\mathfrak{u} \cdot \mathfrak{v}) \cap R$ again

$$\alpha(c) \;=\; \alpha\left(\sum_{k=1}^{n} a_k b_k\right) \;=\; \sum_{k=1}^{n} \alpha(a_k)\alpha(b_k)$$

(ii) Let us denote the set of all $s \in S$ that are finite sums of elements of the form $s_i\,\alpha(a_i)$ where $s_i \in S$ and $a_i \in A$, where $A := \bigcup_\lambda \mathfrak{a}_\lambda$ is the union of all $\mathfrak{a}_\lambda$, by

$$\mathfrak{s} \;=\; \left\{ \sum_{i=1}^{n} s_i\,\alpha(a_i) \;\middle|\; n \in \mathbb{N},\, s_i \in S,\, a_i \in A \right\}$$

We will prove that both sums are identical to this set. In both cases one inclusion is obvious: If $a_i \in \mathfrak{a}_\lambda$ then $s_i\,\alpha(a_i) \in \mathfrak{a}_\lambda S$ and hence any $s \in \mathfrak{s}$ is contained in the sum of all $\mathfrak{a}_\lambda$. Also any $a_i \in A$ is contained in the sum of the $\mathfrak{a}_\lambda$ such that any $s \in \mathfrak{s}$ also is contained in the push-out of the sum of the $\mathfrak{a}_\lambda$. We will see, that the converse inclusions are true, as well and in particular the sums are equal: Consider any element s of the sum of the $\mathfrak{a}_\lambda S$, that is there are some $u_i \in S$ and $h_i \in \mathfrak{a}_{\lambda(i)} S$ such that s is of the form

$$s \;=\; u_1 h_1 + \cdots + u_r h_r$$

By construction any h_i is a sum of elements of the form $v_{i,j}\,\alpha(a_{i,j})$ where $a_{i,j} \in \mathfrak{a}_{\lambda(i)}$ for some

$\lambda(i) \in \Lambda$. That is s is an expression of a form that is contained in $\mathfrak{s}$, since

$$s \;=\; \sum_{i=1}^{r} u_i h_i \;=\; \sum_{i=1}^{r} u_i \sum_{j=1}^{n(i)} v_{i,j}\, \alpha(a_{i,j}) \;=\; \sum_{i=1}^{r}\sum_{j=1}^{n(i)} u_i v_{i,j}\, \alpha(a_{i,j}) \;\in\; \mathfrak{s}$$

Hence the sum of the $\mathfrak{a}_\lambda S$ equals $\mathfrak{s}$. Let us also demonstrate that the push-out of the sum of the $\mathfrak{a}_\lambda$ also is contained in $\mathfrak{s}$: That is we consider any $s \in \mathfrak{a}S$ where $\mathfrak{a}$ is the sum of the $\mathfrak{a}_\lambda$. In particular s is of the form

$$s \;=\; u_1\alpha(a_1) + \cdots + u_r\alpha(a_r)$$

for some $u_i \in S$ and $a_i \in \mathfrak{a} = \langle A \rangle_\mathfrak{i}$. That is there are some $r_{i,j} \in R$ and $a_{i,j} \in \mathfrak{a}_{\lambda(i,j)}$ for some $\lambda(i,j) \in \Lambda$ such that a_i is the sum of the $r_{i,j}a_{i,j}$. And thereby we find that s is contained in $\mathfrak{s}$ again

$$s \;=\; \sum_{i=1}^{r} u_i\, \alpha(a_i) \;=\; \sum_{i=1}^{r} u_i\, \alpha\left(\sum_{j=1}^{n(i)} r_{i,j}a_{i,j}\right) \;=\; \sum_{i=1}^{r}\sum_{j=1}^{n(i)} u_i\, \alpha(r_{i,j})\, \alpha(a_{i,j}) \;\in\; \mathfrak{s}$$

(ii) Let $\mathfrak{a}$ be the intersection of all the $\mathfrak{a}_\lambda$. It remains to prove that any $s \in \mathfrak{a}S$ already is contained in the intersection of all the $\mathfrak{a}_\lambda S$. That is s is of the form

$$s \;=\; u_1\alpha(a_1) + \cdots + u_r\alpha(a_r)$$

for some $u_r \in S$ and $a_i \in \mathfrak{a}$. Fix any $\lambda \in \Lambda$, then $a_i \in \mathfrak{a} \subseteq \mathfrak{a}_\lambda$ such that we have $s \in \mathfrak{a}_\lambda S$, too. But as this is true for any $\lambda \in \Lambda$ we see that s is contained in the intersection of the $\mathfrak{a}_\lambda$ already.

(ii) By definition of the product of ideals $\mathfrak{a} \cdot \mathfrak{b}$ the elements of this ideal are of the form $\sum_i a_i b_i$ for some $a_i \in \mathfrak{a}$ and $b_i \in \mathfrak{b}$. In particular $\alpha(a_i) \in \alpha(\mathfrak{a}) \subseteq \mathfrak{a}S$ and likewise $\alpha(b_i) \in \alpha(\mathfrak{b}) \subseteq \mathfrak{b}S$. As α is a homomorphism of rings, we get

$$\alpha\left(\sum_{i=1}^{n} a_i b_i\right) \;=\; \sum_{i=1}^{n} \alpha(a_i)\alpha(b_i) \;\in\; (\mathfrak{a}S)\cdot(\mathfrak{b}S)$$

Note that the sum is contained in $(\mathfrak{a}S)\cdot(\mathfrak{b}S)$ as this is an ideal in S. That is we have proved $\alpha(\mathfrak{a}\cdot\mathfrak{b}) \subseteq (\mathfrak{a}S)\cdot(\mathfrak{b}S)$ and as $(\mathfrak{a}\cdot\mathfrak{b})S$ is generated by this image set we have found the inclusion from right to left. For the converse inclusion we regard an element $w \in (\mathfrak{a}S)\cdot(\mathfrak{b}S)$ which are of the form [for some $u_k \in \mathfrak{a}S$ and $v_k \in \mathfrak{b}S$]

$$w \;=\; \sum_{k=1}^{n} u_k v_k$$

That is u_k is a finite sum of elements of the form $f_{k,i}\alpha(a_{k,i})$ for some $f_{k,i} \in S$ and $a_{k,i} \in \mathfrak{a}$. Likewise v_k is a finite sum of some $g_{k,j}\alpha(b_{k,j})$ where $g_{k,j} \in S$ and $b_{k,j} \in \mathfrak{b}$. Inserting this into w we find

$$w \;=\; \sum_{k=1}^{n} \left(\sum_{i=1}^{I(k)} f_{k,i}\, \alpha(a_{k,i})\right)\left(\sum_{j=1}^{J(k)} g_{k,j}\, \alpha(b_{k,j})\right) \;=\; \sum_{k=1}^{n}\sum_{i=1}^{I(k)}\sum_{j=1}^{J(k)} f_{k,i}g_{k,j}\, \alpha(a_{k,i}b_{k,j})$$

As $a_{k,i}b_{k,j} \in \mathfrak{a}\cdot\mathfrak{b}$ we hence find that w is an S-linear combination of elements of $\alpha(\mathfrak{a}\cdot\mathfrak{b})$. This

again means, that w is contained in $(\mathfrak{a}\cdot\mathfrak{b})S$ again, by construction of pushed-out ideals.

□

Proof of (8.9):
Let us assume f splits over S in the form $f(t) = \mathrm{lc}(f)(t-s_1)\dots(t-s_n) \in S[t]$ and expand this product denoting the $(k \in \mathbb{N})$-th coefficient of $(t-s_1)\dots(t-s_n)$ by

$$e_k(s_1,\dots,s_n) \;:=\; \left(\prod_{k=1}^{n}(t-s_k)\right)[k]$$

By the theorem of Vieta (7.66) we even know the exact shape of $e_k(s_1,\dots,s_n)$ to be the $(n-k)$-th elementary symmetric polynomial in n-variables $e_k(s_1,\dots,s_n) = (-1)^{n-k}s^{(n)}_{n-k}(s_1,\dots,s_n)$ but this is irrelevant here. We only need, that $e_k(s_1,\dots,s_n)$ is a uniquely determined polynomial in the s_k again. By remark (8.8) $\mathrm{lc}(f)(t-s_1)\dots(t-s_n) = f$ has to be decoded in the following form

$$\forall\, k \in \mathbb{N} \;:\; \alpha(\mathrm{lc}(f))\cdot e_k(s_1,\dots,s_n) \;=\; \alpha(f[k])$$

As β is a homomorphism of rings, it commutes with polynomials and hence we may insert $e_k(s_1,\dots,s_n)$ into β and thereby find the following identity

$$\prod_{k=1}^{n}\big(t-\beta(s_k)\big) \;=\; e_k\big(\beta(s_1),\dots,\beta(s_n)\big) \;=\; \beta\big(e_k(s_1,\dots,s_n)\big)$$

If we insert $\alpha(f[k])$ into β we can again use its homomorphism property and the equation above, to find $f[k] = \mathrm{lc}(f)(t-\beta(s_1))\dots(t-\beta(s_n))$ as an equation in the ring extension $T[t] : R[t]$ induced by $\beta\alpha : R \to T$. In particular f splits over T, too, as we can compute

$$\beta\alpha(f[k]) \;=\; \beta\alpha(\mathrm{lc}(f))\cdot\beta\big(e_k(s_1,\dots,s_n)\big) \;=\; \beta\alpha(\mathrm{lc}(f))\cdot\prod_{k=1}^{n}\big(t-\beta(s_k)\big)$$

□

Proof of (8.24):

(i) By definition any polynomial $f \in R[I]$ only has finitely many non-zero coefficients, and therefore $A(f) := \{\, \alpha \in \mathbb{N}^{\oplus I} \mid f[\alpha] \neq 0 \,\}$ is a finite set. Also $I(\alpha) := \{\, i \in I \mid \alpha_i \neq 0 \,\}$ is a finite set for any $\alpha \in \mathbb{N}^{\oplus I}$. In combination

$$\Omega \;:=\; \bigcup\{\, I(\alpha) \mid \alpha \in A(f) \,\}$$

is a finite subset of I. If $f[\alpha]\,t^\alpha$ is a non-zero term of f then $t^\alpha = \prod_i t_i^{\alpha_i}$ only contains those t_i that belong to some $i \in \Omega$ and therefore $f \in \iota^I_\Omega(R[\Omega])$. And as this is true for any $f \in R[I]$, we get the inclusion from left to right. The converse inclusion is trivial, however.

(ii) By construction of the canonical maps $\iota^J_I(f) = f\,1_{R[J]}$ for any $f \in R[I]$ and under ι^K_J this is mapped to $f\,1_{R[J]}\,1_{R[K]} = f\,1_{R[K]} = \iota^K_I(f)$. Thus we already have $\iota^K_I = \iota^K_J\iota^J_I$. The homomorphism π^J_I exists and is uniquely determined, as it is an evaluation homomorphism, defined on the generating set $\{\, t_j \mid j \in J \,\}$ of $R[J]$, refer to (7.14). Now for any $i \in I$ we get $\pi^J_I\iota^J_I(t_i) = \pi^J_I(t_i) = t_i$. And as both

π_I^J and ι_I^J are homomorphisms of R-algebras this implies $\pi_I^J\iota_I^J(a) = a$ for any $a \in R[I]$, which is property (2). In particular π_I^J is surjective, by (0.10.(a)). Now consider some $f \in \mathfrak{a}\,R[J]$, that is f is of the form $f = f_1\iota_I^J(a_1) + \cdots + f_r\iota_I^J(a_r)$ for some $f_l \in R[J]$ and $a_l \in \mathfrak{a}$. Then we also get property (3) from the computation

$$\pi_I^J(f) \;=\; \pi_I^J\left(\sum_{l=1}^{r} f_l\,\iota_I^J(a_l)\right) \;=\; \sum_{l=1}^{r} \pi_I^J(f_l)\,\pi_I^J\iota_I^J(a_l) \;=\; \sum_{l=1}^{r} \pi_I^J(f_l)\,a_l \;\in\; \mathfrak{a}$$

(iii) Actually this already has been proved in (ii): As $\widehat{a} = \iota_I^J(a)$ we get $\pi_I^J(\widehat{a}) = \pi_I^J\iota_I^J(a) = a$ and hence we only need to apply π_I^J to the equation $\widehat{a} = f_1\widehat{a}_1 + \cdots + f_r\widehat{a}_r$ and let $b_l := \pi_I^J(f_l)$. If we redo the last computation, we thereby find

$$a \;=\; \pi_I^J(\widehat{a}) \;=\; \pi_I^J\left(\sum_{l=1}^{r} f_l\,\widehat{a}_l\right) \;=\; \sum_{l=1}^{r} \pi_I^J(f_l)\,\pi_I^J(\widehat{a}_l) \;=\; \sum_{l=1}^{r} b_l\,a_l$$

(iv) First note that by (8.18) $(\mathfrak{a}\,R[J])R[K] = \mathfrak{a}\,R[K]$ is generally true in any ring extension. Thus the inclusion $\mathfrak{a}\,R[J] \subseteq (\mathfrak{a}\,R[K]) \cap R[J]$ is a general truism, by (8.15), as well. It remains to check the converse inclusion $(\mathfrak{a}\,R[K]) \cap R[J] \subseteq \mathfrak{a}\,R[J]$. To do this we first recollect the definitions of the transferred ideals

$$(\mathfrak{a}\,R[K]) \cap R[J] \;=\; (\iota_J^K)^{-1}\big(\langle\,\iota_I^K(\mathfrak{a})\rangle\big)$$

That is for any element $a \in (\mathfrak{a}\,R[K]) \cap R[J]$ there are some $f_1, \ldots, f_r \in R[K]$ and $a_1, \ldots, a_r \in \mathfrak{a}$ such that [where we use the abbreviations $\widehat{a} = \iota_J^K(a)$ and $\widehat{a}_l = \iota_I^K(a_l)$] a is of the following form

$$\widehat{a} \;=\; f_1\widehat{a}_1 + \cdots + f_r\widehat{a}_r$$

Note that $\iota_J^K\iota_I^J = \iota_I^K$ such that $\widehat{a}_l = \iota_J^K(\iota_I^J(a_i))$. Now by virtue of (ii) the above equation implies that there are some polynomials $b_1, \ldots, b_r \in R[J]$ such that

$$a \;=\; b_1\,\iota_I^J(a_1) + \cdots + b_r\,\iota_I^J(a_r) \;\in\; \mathfrak{a}\,R[J]$$

In the second equality the inclusion $\mathfrak{b} \subseteq (\mathfrak{b}\,R[K]) \cap R[J]$ is (8.15) again. And by (8.18) we also have $(\mathfrak{u} \cap R[J]) \cap R[I] = \mathfrak{u} \cap R[I]$ in general, for any ideal $\mathfrak{u} \trianglelefteq_{\mathrm{i}} R[K]$, in particular for $\mathfrak{u} := \mathfrak{b}\,R[K]$. Hence we get $\mathfrak{b} \cap R[I] \subseteq (\mathfrak{b}\,R[K]) \cap R[J] \cap R[I] = (\mathfrak{b}R[K]) \cap R[I]$. So we only need to check the converse inclusion and start with some element $a \in (\mathfrak{b}\,R[K]) \cap R[I]$. That is $\widehat{a} = f_1\widehat{a}_1 + \cdots + f_r\widehat{a}_r$ for some $f_1, \ldots, f_r \in R[K]$ and $a_1, \ldots, a_r \in \mathfrak{b}$, where $\widehat{a} = \iota_I^K(a)$ and $\widehat{a}_l = \iota_J^K(a_l)$. But then, by (ii) again, we find $a \in \mathfrak{b} \cap R[I]$ from

$$\iota_I^J(a) \;=\; b_1\,a_1 + \cdots + b_r\,a_r \;\in\; \mathfrak{b}$$

(v) For ease of notation we regard $R[I] \subseteq R[J]$ as a subset under ι_I^J. Then for any $\alpha \in \mathbb{N}^{\oplus H}$ and $g[\alpha] \in \mathfrak{a}$ it is clear that $g[\alpha]t^\alpha \in \mathfrak{a}\,R[J]$ and hence $\mathfrak{a}[H] \subseteq \mathfrak{a}\,R[J]$. Conversely, if $g \in \mathfrak{a}\,R[J]$, there g is of the form $g = g_1a_1 + \cdots + g_ra_r$ for some $g_l \in R[J]$ and $a_l \in \mathfrak{a}$. Let us now write $g_l \in R[J]$

as an element of $S[H]$, which is

$$g_l \;=\; \sum_{(\alpha,\beta)\in\mathbb{N}^{\oplus(H\cup I)}} g_l[\alpha,\beta]\,t^{(\alpha,\beta)} \;=\; \sum_{\alpha\in\mathbb{N}^{\oplus H}} \underbrace{\left(\sum_{\beta\in\mathbb{N}^{\oplus I}} g_l[\alpha,\beta]\,t^{\beta}\right)}_{g_l[\alpha]\in S} t^{\alpha}$$

Then it becomes clear that $g \in \mathfrak{a}[H]$, as we can write it in the following form

$$g \;=\; \sum_{l=1}^{r} g_l\,a_l \;=\; \sum_{l=1}^{r}\left(\sum_{\alpha\in\mathbb{N}^{\oplus H}} g_l[\alpha]\,t^{\alpha}\right)a_l \;=\; \sum_{\alpha\in\mathbb{N}^{\oplus H}} \underbrace{\left(\sum_{l=1}^{r} g_l[\alpha]\,a_l\right)}_{\in\mathfrak{a}} t^{\alpha}$$

Thus we also have $\mathfrak{a}\,R[J] \subseteq \mathfrak{a}[H]$ and hence the equality. Let us now prove the isomorphism property. We start by taking a look at the following homomorphism of R-algebras

$$\varrho \;:\; R[J] \;\twoheadrightarrow\; \left(R[I]\,\big/\,\mathfrak{a}\right)[H] \;:\; g \;\mapsto\; \sum_{\alpha\in\mathbb{N}^{\oplus H}} \big(g[\alpha]+\mathfrak{a}\big)t^{\alpha}$$

It is clear, that ϱ is surjective, as $R[I] \twoheadrightarrow R[I]/\mathfrak{a} : g[\alpha] \mapsto g[\alpha]+\mathfrak{a}$ is surjective. So let us take a look at the kernel of ϱ. We find $\operatorname{kn}(\varrho) = \mathfrak{a}[H] = \mathfrak{a}\,R[J]$ from

$$\begin{aligned}
\varrho(g) = 0 \quad &\Longleftrightarrow \quad \forall\,\alpha\in\mathbb{N}^{\oplus H} \;:\; g[\alpha]+\mathfrak{a} = 0\\
&\Longleftrightarrow \quad \forall\,\alpha\in\mathbb{N}^{\oplus H} \;:\; g[\alpha]\in\mathfrak{a}\\
&\Longleftrightarrow \quad g \;\in\; \mathfrak{a}[H]
\end{aligned}$$

Thus ϱ induces the isomorphism given in the claim. Now suppose $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R[I]$ is a prime ideal, then $R[I]/\mathfrak{p}$ is an integral domain and therefore $(R[I]/\mathfrak{p})[H]$ is an integral domain, too. Due to the above isomorphism this means, that $R[J]/(\mathfrak{p}\,R[J])$ is an integral domain, too. And this again tells us that $\mathfrak{p}\,R[J] \trianglelefteq_{\mathrm{i}} R[J]$ is a prime ideal.

(vi) Let us first prove, that these ideals truly form an ascending chain again, that is for $n \geq 1$ we get $(\mathfrak{a}\cap R[I_{n-1}])\,R[J] \subseteq (\mathfrak{a}\cap R[I_n])\,R[J]$. As always $f \in (\mathfrak{a}\cap R[I_{n-1}])\,R[J]$ f is of the form

$$f \;=\; f_1\,\iota^J_{I_{n-1}}(a_1) + \cdots + f_r\,\iota^J_{I_{n-1}}(a_r)$$

for some $f_l \in R[J]$ and $a_l \in \mathfrak{a}\cap R[I_{n-1}]$. The latter is $\iota^J_{I_{n-1}}(a_l) \in \mathfrak{a}$ so let us define $\widehat{a}_l := \iota^{I_n}_{I_{n-1}}(a_l)$ such that $\iota^J_{I_n}(\widehat{a}_l) = \iota^J_{I_{n-1}}(a_l)$. Then we find

$$f \;=\; \sum_{l=1}^{r} f_l\iota^J_{I_{n-1}}(a_l) \;=\; \sum_{l=1}^{r} f_l\iota^J_{I_n}(\widehat{a}_l) \;\in\; \big(\mathfrak{a}\cap R[I_n]\big)\,R[J]$$

It remains to verify the capstone property of $\mathfrak{a}$: The inclusion $(\mathfrak{a}\cap R[I_n])\,R[J] \subseteq \mathfrak{a}$ has been proved in (8.15) and hence we find the inclusion "$\subseteq$" for the (infinite) sum. Now for the converse inclusion "$\supseteq$": Given any $f \in \mathfrak{a} \subseteq R[J]$ we know by (i) that there is a finite subset $\Omega \subseteq J$ such that $f \in \iota^J_\Omega(R[\Omega])$. Now, as Ω is finite and the I_n exhaust J there is a finite level $n \in \mathbb{N}$ such that $\Omega \subseteq I_n$. That is there is some $a \in R[I_n]$ such that $f = \iota^J_{I_n}(a)$. As $f \in \mathfrak{a}$ this means $a \in \mathfrak{a}\cap R[I_n]$

and thereby $f = \iota^J_{I_n}(a) \in (\mathfrak{a} \cap R[I_n])R[J]$.

□

Proof of (8.28):

- Let us first consider the case that $\{ s_i \mid i \in I \} \subseteq S$ generates S as an R module and consider any $q \in Q$. As π is surjective there is some $s \in S$ such that $\pi(s) = q$. This $s \in S$ has a representation as an R-linear combination in terms of the s_i

$$s \;=\; \sum_{i \in I} r_i s_i$$

for some $r_i \in R$ of which only finitely many are non-zero. If we insert this into π and use the properties of π as a homomorphsim of rings, we find that q can be written as the linear combination

$$q \;=\; \pi(s) \;=\; \sum_{i \in I} \pi(r_i)\pi(s_i)$$

As $\pi(r_i) \in \pi(R) \subseteq P$ this is a P-linear combination. As $q \in Q$ has been arbitrary, this means that $\{ \pi(s_i) \mid I \}$ generates Q as a P-module. And in particular the rank of Q as a P-module cannot exceed the rank of S as an R-module

$$[Q : P] \;\leq\; [S : R]$$

- Now say $\{ s_i \mid i \in I \} \subseteq S$ generates S as an R-algebra. That is for any $x \in S$ there are finitely many $s_1, \ldots, s_n \in \{ s_i \mid i \in I \}$ and there is a polynomial $f \in R[t_1, \ldots, t_n]$ such that x can be written as [where $s := (s_1, \ldots, s_n) \in S^n$]

$$x \;=\; f(s_1, \ldots, s_n) \;=\; \sum_{\alpha \in \mathbb{N}^n} f[\alpha]\, s^\alpha$$

If $q \in Q$ is any element again, then we choose some $x \in S$ with $\pi(x) = s$, which is possible, as π is surjective, again. And as above all we need to do is insert this equation into π and use the homomorphism properties

$$q \;=\; \pi(x) \;=\; \sum_{\alpha \in \mathbb{N}^n} \pi\big(f[\alpha]\big)\, \pi(s)^\alpha$$

where $\pi(s) = (\pi(s_1), \ldots, \pi(s_n))$ of course. Again we have $\pi(f[\alpha]) \in \pi(R) \subseteq P$, such that q is a polynomial with coefficients in P in some elements from $\{ \pi(s_i) \mid I \}$. As q has been taken arbitrarily, this means $\{ \pi(s_i) \mid I \}$ generates Q as a P-algebra. And if $S : R$ is finitely generated, then we can choose I to be finite, such that $Q : P$ then is finitely generated, too.

- Now suppose $S : R$ is integral, then we need to show, that $Q : P$ is integral, too. Consider any $q \in Q$ and choose $s \in S$ with $\pi(s) = q$, one more. As $S : R$ is integral, there is some $n \in \mathbb{N}$ and there are $a_0, \ldots, a_{n-1} \in R$ such that

$$s^n + \sum_{k=0}^{n-1} a_k s^k \;=\; 0$$

As always inset this equation into π use the properties of a homomorphism of rings, recall $q = \pi(s)$ and $\pi(a_k) \in \pi(R) \subseteq P$, then we find then q also is integral over P, as it satisfies the equation

$$q^n + \sum_{k=0}^{n-1} \pi(a_k) q^k \;=\; 0$$

□

Proof of (8.29):

(i) As $x \in S$ is integral over R there is a monic polynomial $f \in R[t]$ such that $f(x) = 0$. In particular $f \neq 0$, as f is monic and $\deg(f) \geq 1$, as $f(x) = 0$. Let $n+1 := \deg(f)$ and $k := \operatorname{ord}(f)$ that is $f[k] \neq 0$ but for any $0 \leq j < k$ we have $f[j] = 0$. In other words we write f in the form

$$f(t) \;=\; t^{n+1} + f[n]t^n + \cdots + f[k]t^k \;=\; t^k \left(t^{n+1-k} + f[n]t^{n-k} + \cdots + f[k]t^0 \right)$$

As $x \in \text{NZD}(R)$ is a non-zero-divisor and $f(x) = 0$ this means that the above polynomial in brackets already has to vanish at x. And as $f[k] \neq 0$ we have found a monic polynomial $m \in R[t]$ such that $m(x) = 0$ but $m(0) = f[k] \neq 0$, as claimed

$$m(t) \;:=\; t^{n+1-k} + f[n]t^{n-k} + \cdots + f[k+1]t + f[k]$$

(ii) If $a \in R^*$ then $\alpha(a) \in S^*$ and $\alpha(a)^{-1} = \alpha(a^{-1})$ have already been shown in (1.76.(ii)). So conversely assume $u = \alpha(a) \in S^*$ that is, there is some $u^{-1} \in S$, such that $u^{-1}u = 1_S$. As $S : R$ is integral there is an equation of the form

$$\left(u^{-1}\right)^{n+1} + a_n \left(u^{-1}\right)^n + \cdots + a_1 u^{-1} + a_0 \;=\; 0$$

for some coefficients $a_k \in R$. Let us multiply this equation by u^n (from the right, but this is irrelevant), then only one u^{-1} remains and hence we can turn this into

$$u^{-1} \;=\; -\left(a_n + \cdots + a_1 u^{n-1} + a_0 u^n \right)$$

However $u = \alpha(a) \in \alpha(R) = R\,1_S$ and $\alpha(R)$ is an R-subalgebra of S. Then the equation above implies $u^{-1} \in \alpha(R)$, too, say $u^{-1} = \alpha(b)$. Then $\alpha(ab) = \alpha(a)\alpha(b) = uu^{-1} = 1_S = \alpha(1_R)$. As α is injective we get $ab = 1_R$ and hence $a \in R^*$ with inverse $a^{-1} = b$.

(iii) Suppose there was some $x \in \mathfrak{u}$ such that also $x \in \text{NZD}(S)$. Then by (i) we find some $m \in R[t]$ such that $m(x) = 0$ but $m(0) \neq 0$. Let $\alpha : R \to S : a \mapsto a1_S$ be the structural homomorphism again, that is $as = \alpha(a) \cdot s$ for any $a \in R$, $s \in S$.

$$0 \;=\; m(x) \;= x^{n+1} + \sum_{k=1}^{n} \alpha(m[k]) \cdot x^k + \alpha(m[0])$$

Then, as $x \in \mathfrak{u}$, we find that $\alpha(m[0])$ is contained in $\mathfrak{u}$ from the following equation, below. But this means $m[0] \in \mathfrak{u} \cap R = 0$ such that $m(0) = m[0] = 0$. But this contradicts $m(0) \neq 0$ and therefore,

there could not have been any $x \in \mathfrak{u} \cap \text{NZD}(R)$ and hence $\mathfrak{u} \subseteq \text{ZD}(R)$.

$$\alpha(m[0]) \;=\; -x\left(x^n + \sum_{k=1}^{n} \alpha(m[k]) \cdot x^{k-1}\right) \;\in\; \mathfrak{u}$$

(iv) Let us abbreviate $a := \mathfrak{u} \cap R$. We have already seen in (8.19.(i)) that this is a well-defined ring extension and that $\overline{\alpha}$ is injective, in this case. It remains to verify, that $S/\mathfrak{u} : R/\mathfrak{a}$ is integral again. So consider any $x + \mathfrak{u}$, as $x \in S$ there is a monic polynomial $m \in R[t]$ such that $m(x) = 0$. Inserting $m(x)$ into the canonical homomorphism $x \mapsto x + \mathfrak{u}$ we find

$$\begin{aligned} 0 + \mathfrak{u} \;&=\; m(x) + \mathfrak{u} \;=\; x^{n+1} + \sum_{k=0}^{n} \alpha(m[k]) \cdot x^k + \mathfrak{u} \\ &=\; (x+\mathfrak{u})^{n+1} + \sum_{k=0}^{n} \big(\alpha(m[k]) + \mathfrak{u}\big) \cdot (x+\mathfrak{u})^k \\ &=\; (x+\mathfrak{u})^{n+1} + \sum_{k=0}^{n} \big(\overline{\alpha}(m[k] + \mathfrak{a})\big) \cdot (x+\mathfrak{u})^k \end{aligned}$$

That is $x + \mathfrak{u} \in S/\mathfrak{u}$ satisfies the monic polynomial $t^{n+1} + (m[n] + \mathfrak{a})t^n + \cdots + (m[0] + \mathfrak{a}) \in R/\mathfrak{a}[t]$ and as x has been arbitrary, this means, that $S/\mathfrak{u}/R/\mathfrak{a}$ is integral, again.

(v) Consider any $x/u \in U^{-1}S$, as $x \in S$ and $S : R$ is integral there is a monic polynomial $f \in R[t]$ such that $f(x) = 0$. Say $n + 1 := \deg(f)$, then we define another monic polynomial over $U^{-1}R$:

$$g(t) \;:=\; t^{n+1} + \sum_{k=0}^{n} \frac{f[k]}{u^{n+1-k}}\, t^k$$

Then the following computation shows $g(x/u) = 0 \in U^{-1}S$ and as x/u is arbitrary this shows that the ring extension $U^{-1}S : U^{-1}R$ is integral, too:

$$g\left(\frac{x}{u}\right) \;=\; \frac{x^{n+1}}{u^{n+1}} + \sum_{k=0}^{n} \frac{f[k]}{u^{n+1-k}} \frac{x^k}{u^k} \;=\; \frac{1}{u^{n+1}}\left(t^{n+1} + \sum_{k=0}^{n} f[k]\, t^k\right) \;=\; \frac{f(x)}{u^{n+1}} \;=\; \frac{0}{u^{n+1}}$$

(vi) Let us first prove that $\{1, t, \ldots, t^{n-1}\}$ is a generating set of $R[t]$ as an $R[f]$-module. That is we consider any $g \in R[t]$ and need to find $g_i \in R[f]$ such that

$$g \;=\; g_0 + g_1 t + \cdots + g_{n-1} t^{n-1}$$

We do this by induction on the degree of g: If $\deg(g) < n$ then the claim is obvious, as we can take the $g_i = g[i] \in R$. If $\deg(g) \geq n$ we use division with remainder to write g as $g = qf + r$ for some q, $r \in R[t]$ with $\deg(r) < \deg(f) = n$. As $\deg(q) < \deg(g)$ we may use the induction hypothesis to write q as a linear combination $q = q_0 + q_1 t + \cdots + q_{n-1} t^{n-1}$, then

$$g \;=\; qf + r \;=\; \sum_{i=0}^{n-1} \big(q_i f + r[i]\big) t^i$$

and $g_i := q_i f + r[i] \in R[f]$ again. Thus g is an $R[f]$-linear combination over the t^i. It remains to

prove, that the t^i also are $R[f]$-linearly independent. To do this we have to consider any $g_i \in R[t]$ such that $g_0(f) + g_1(f)t + \cdots + g_{n-1}(f)t^{n-1} = 0$. Let us take those g_i whose sum of degrees is minimal. As $g_0(f) + g_1(f)t + \cdots + g_{n-1}(f)t^{n-1} = 0$ we also get

$$0 + pE[x] \;=\; \sum_{i=0}^{n-1} g_i(f)t^i + fR[t] \;=\; \sum_{i=0}^{n-1} g_i(0)t^i + fR[t]$$

and as $\deg(f) = n$ this means $g_i(0) = 0$ for any $i \in 0 \ldots n-1$. But this means $t \mid g_i$ and hence $g_i(f) = fh_i(f)$ for some $h_i \in R[t]$. Thus we may scratch f from the equation and find another equation $h_0(f) + h_1(f)t + \cdots + h_{n-1}(f)t^{n-1} = 0$ again. But the sum of the degrees of the h_i is n less, in contradiction to the minimality of the degrees of the g_i. Thus we had $g_i = 0$ for any $i \in 0 \ldots n-1$ in the first place and this is the linear independence of $\{ 1, t, \ldots, t^{n-1} \}$.

□

Proof of (8.30):

(i) Let m be a monic polynomial, $n := \deg(m)$ and $X := \{ x^k \mid 0 \leq k < n \}$. Then we need to show that any element $y \in R[x]$ can be written as a linear combination in terms of X. To see this note that y is of the form $y = f(x)$ for some polynomial $f \in R[t]$. As m is monic we may use division with remainder (2.67) to find polynomials q and $r \in R[t]$ such that $f = qm + r$ and $\deg(r) < n$. Then we find $y = r(x)$ from $y = f(x) = q(x) \cdot m(x) + r(x) = q(x) \cdot 0 + r(x) = r(x)$. Now due to the degree of r we have

$$y \;=\; r(x) \;=\; \sum_{k=0}^{n-1} r[k]x^k \;\in\; \mathrm{Lh}_R(X)$$

(ii) In case $n = 1$ this is the statement of (i) precisely. In case $n \geq 2$ we use induction on n: Let us denote $P_0 := R[x_1, \ldots, x_{n-1}]$ then $P = P_0[x_n]$ according to (8.5). And as x_n is integral over R it also is integral over P_0, since $R \subseteq P_0$. So by (i) again, we have

$$[P : P_0] \;=\; [P_0[x_n] : P_0] \;<\; \infty$$

By induction hypothesis we also have $[P_0 : R] < \infty$. Combining these we may use the degree formula (8.7.(iv)) to find the claim

$$[P : R] \;\leq\; [P : P_0] \cdot [P_0 : R] \;<\; \infty$$

(iii) Let $n := [S : R]$ be the degree of the extension and let $\{ s_1, \ldots, s_n \} \subseteq S$ be a generating set of S as an R-module. For any $i \in 1 \ldots k$ choose a representation of xs_i in term of this generating set

$$xs_i \;=\; \sum_{j=1}^{n} a_{i,j}s_j$$

and define the matrix $A := (a_{i,j}) \in \mathrm{mat}_n(R)$. For any other element $y = b_1s_1 + \cdots + b_ns_n$ we let $b := (b_1, \ldots, b_n)$ and thereby get

$$xy \;=\; x\sum_{i=1}^{n} b_is_i \;=\; \sum_{i=1}^{n} b_ixs_i \;=\; \sum_{i=1}^{n}\sum_{j=1}^{n} b_ia_{i,j}s_i \;=\; \sum_{i=1}^{n} [Ab]_is_i$$

By induction it is clear, that $x^k y = [A^k b]_1 s_1 + \cdots + [A^k b]_n s_n$. Thus for any polynomial $f \in R[t]$ we have $f(x)y = [f(A)b]_1 s_1 + \cdots + [f(A)b]_n s_n$. Let $m := c_A$ be the characteristic polynomial of A - recall that this is $m(t) = \det(t\mathbb{1}_n - A)$. Then the Cayley-Hamilton theorem (5.44) tells us, that m is a monic polynomial of degree n satisfying $m(A) = 0 \in \mathrm{mat}_n(R)$. By what we have argued this means that $m(x)y = [m(A)b]_1 s_1 + \cdots + [m(A)b]_n s_n = 0$. By choosing $y = 1_S$ we find that $m(x) = 0$ and hence we have found the monic polynomial required.

(iii) *Alternate proof, that $S : R$ is algebraic, only*: Let $n := [S : R]$ be the degree of the extension. Given any $x \in S$ we consider the set $X := \{\, x^k \mid 0 \leq k \leq n \,\}$. If $\#X \leq n$ then there are some $i < j \in 0 \ldots n$ such that $x^i = x^j$. In this case we may take $f(t) := t^j - t^i \in R[t]$ to find $f(x) = 0$. If $\#X = n + 1$ then we may invoke lemma (3.99.(i)) to find that X is R-linearly dependent. That is there are $a_k \in R$ (not all zero) such that

$$a_n x^n + \cdots + a_1 x + a_0 \cdot 1 \quad = \quad 0$$

Thus we have found a polynomial $f \in R[t]$ of degree n at most, by taking $f[k] := a_k$ such that $f(x) = 0$. And as not all a_k are zero we have $f \neq 0$ and this means x is algebraic over R.

(iv) Consider any $s \in S$, as $S = R[X]$ there are finitely $x_1, \ldots, x_n \in X$ such that $s \in R[x_1, \ldots, x_n]$, according to the construction (8.4). As all the x_i are integral by assumption $R[x_1, \ldots, x_n]$ is finite, due to (ii). But a finite extension is integral by (iii), that is there is a monic polynomial $m \in R[t]$ such that $m(s) = 0$. Yet as s has been arbitrary, this means $S : R$ is integral.

(v) If $S : R$ is integral and finitely generated, then it is precisely the statement of (ii) that $S : R$ also is finite. Conversely if $S : R$ is finite, say $S = \mathrm{Lh}_R\{\, s_1, \ldots, s_k \,\}$ for some $s_1, \ldots, s_k \in S$, then clearly $S = R[s_1, \ldots, s_k]$, as we have the chain of inclusions

$$S \;=\; \mathrm{Lh}_R\{\, s_1, \ldots, s_k \,\} \;\subseteq\; R[s_1, \ldots, s_k] \;\subseteq\; S$$

Hence $S : R$ is finitely generated and also integral, according to (iii).

(vi) For any $a \in R$ it is clear that $m(t) := t - a \in R[t]$ satisfies $m(a1_S) = 0$ and hence $a \in \overline{R}$, such that $R\,1_S \subseteq \overline{R}$. In particular $1_S \in \overline{R}$. It remains to prove, that $\overline{R}$ is a sub-ring if S: Given $x, y \in \overline{R}$ we see that $R[x, y]$ is finitely generated by integral elements and hence $R[x, y] : R$ is finite by (ii). Then again $R[x, y] : R$ is integral, by (iii). In particular $x + y$ and $xy \in R[x, y]$ are integral, that is $x + y$, $xy \in \overline{R}$ and hence this is also is a sub-ring of S.

(vi) Nota the proof of $\int(S : \overline{R}) = \overline{R}$ already uses the next lemma (8.31). Note however, that in the proof of this lemma we did not use this property. We only placed this property here, in order to present the statements in thematic order. No logical loop has been made.

Let us now prove $\int(S : \overline{R}) = \overline{R}$. That is we regard some $s \in S$ such that s is integral over $\overline{R}$ and have to prove that s already is integral over R. Yet as s is integral over $\overline{R}$, the extension $\overline{R}[s] : \overline{R}$ is finite, by (i) and hence integral by (iii). Also $\overline{R} : R$ is integral (by definition of $\overline{R}$) such that from (8.31.(ii)) we find, that $\overline{R}[s] : R$ is integral. In particular s is integral over R, which is $s \in \overline{R}$.

(vii) Take a look at the homomorphism $\varepsilon_x : E[t] \twoheadrightarrow E[x] : f \mapsto f(x)$, which is surjective, by definition of $E[x]$ and let us denote its kernel by $\mathfrak{v}_x := \mathrm{kn}(\varepsilon_x) = \{\, f \in E[t] \mid f(x) = 0 \,\}$. Then we find an induced homomorphism

$$E[t] \big/ _{\mathfrak{v}_x} \xrightarrow{\sim} E[x] \ : \ f + \mathfrak{v}_x \mapsto f(x)$$

As $E[x] \leq_{\mathrm{r}} E[t]$ is a sub-ring, $E[t]$ is a prime ideal, by (2.12). And as x is algebraic over E there is some $f \in \mathfrak{v}_x$ with $f \neq 0$. As $E[t]$ is a PID, any non-zero prime ideal $\mathfrak{v}_x$ of $E[t]$ is maximal, by (2.71) and (2.79). But as $\mathfrak{v}_x$ is maximal, the quotient ring $E[t]/\mathfrak{v}_x$ is a field, by (2.5). And due to the above isomorphism, this means $E[x]$ is a field.

(viii) In (a) $\implies$ (b) we first prove, that S is torsion-free, as an R-module: Consider any $a \in R$ and $s \in S$ such that $as = 0$. If $a = 0$ there is nothing to do, else for $a \neq 0$ - as R is a field - there is an inverse a^{-1} of a such that we get $s = 0$ from the computation

$$0 \ = \ a^{-1}0 \ = \ a^{-1}(as) \ = \ (a^{-1}a)s \ = \ 1_R s \ = \ s$$

It remains to prove, that S even is a field: Consider any $x \in S$ such that $x \neq 0$. As $S : R$ is integral we can choose a minimal $n \in \mathbb{N}$ such that there are some $a_k \in R$ such that we have an equation of the form

$$a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0 1_S \ = \ 0$$

(in fact, there even is an equation with $a_n = 1$). As n is minimal we clearly have $a_n \neq 0$. Suppose we had $a_0 = 0$ then we might pull out an x to arrive at $x(a_n x^{n-1} + \cdots + a_2 x + a_1 1_S) = 0$. But as $x \neq 0$ and S is an integral domain this would mean $a_n x^{n-1} + \ldots a_2 x + a_1 1_S = 0$, in contradiction to n being minimal, as well. Hence we have $a_0 \neq 0$ and, as R is a field, this means a_0 has an inverse $a_n^{-1} \in R$. Thus the equation above can be turned into

$$1_S \ = \ -a_0^{-1}\left(a_n x^n + \cdots + a_2 x^2 + a_1 x\right) \ = \ -a_0^{-1}\left(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_2 x + a_1\right) x$$

That is we have found $-a_0^{-1}(x^{n-1} + \ldots a_2 x + a_1)$ to be the inverse element of x. And as x has been arbitrary, this means any $x \in S$ is invertible and hence S is a field.

(viii) In (b) $\implies$ (a) it is clear, that S is an integral domain, as we even assume S to be a field. Now consider any $a \in R$ such that $a1_S = 0$. As $S \neq 0$ we have $1_S \neq 0$ and as S is torsion-free, as an R-module, this implies $a = 0$. That is we have established the implication

$$a1_S \ = \ 0 \quad \Longrightarrow \quad a \ = \ 0$$

In other words: If we start with some $a \neq 0$ we have $x := a1_S \in S$ is $x \neq 0$, non-zero, again. And as S is a field x thereby has an inverse $y = x^{-1} \in S$, that is $xy = 1_S$. But as $S : R$ is integral there also is an equation of the form

$$y^{n+1} + a_n y^n + \cdots + a_2 y^2 + a_1 y + a_0 1_S \ = \ 0$$

Multiplying this equation by x^n, bringing all but y on the right-hand side and replacing x^{n-k} by

$a^{n-k}1_S$ again, we arrive at

$$\begin{aligned} y &= -\left(a_n 1_S + \cdots + a_2 x^{n-2} + a_1 x^{n-1} + a_0 x^n\right) \\ &= -\left(a_n + \cdots + a_2 a^{n-2} + a_1 a^{n-1} + a_0 a^n\right) 1_S \end{aligned}$$

That is we find that y is of the form $y = b1_S$ for some $b \in R$ and thereby $1_S = xy = (a1_S)(b1_S) = (ab)1_S$. Now $(ab - 1_R)1_S = 0$ yields $ab = 1_R$ by the implication above and hence $a \in R^*$ with inverse $a^{-1} = b$. As a has been arbitrary this shows, that R is a field.

(ix) If x is integral over $\mathfrak{a}$ then in particular x is integral (over R), as $\mathfrak{a} \subseteq R$. That is $x \in \overline{R}$ but by definition this means that there are some $a_k \in \mathfrak{a}$ such that we have a relation of the form

$$x^n = -\sum_{k=0}^{n-1} a_k x^k \in \mathfrak{a}\overline{R}$$

As $x \in \overline{R}$ this means, that the sum is contained in $\mathfrak{a}\overline{R}$ and hence x in the the radical thereof. Conversely suppose x is contained in the radical of this ideal, that is $x^n \in \mathfrak{a}\overline{R}$ for some $n \in \mathbb{N}$. Then by definition of the push-out there are $a_1, \ldots, a_m \in \mathfrak{a}$ and $x_1, \ldots, x_m \in \overline{R}$ such that

$$x^m = a_1 x_1 + \cdots + a_m x_m$$

Let $M := R[x_1, \ldots, x_m]$, then we have $M \subseteq \overline{R}$ by (vi). And as all the x_i are integral over R and we only took finitely many x_i the R-module M is finitely generated, due to (ii). Clearly we have $x_i M \subseteq M$, by construction and hence

$$x^n M \subseteq \sum_{i=1}^{m} a_i x_i M \subseteq \sum_{i=1}^{m} a_i M \subseteq \mathfrak{a}M$$

as the $a_i \in \mathfrak{a}$. Also $x^m \in M$, by construction again. We now define an R-module-endomorphism $\varphi : M \to M$ by letting $\varphi(y) := x^n y$. Then we have $\varphi(y) \in x^n M \subseteq \mathfrak{a}M$ and as this is true for any $y \in M$ we have $\varphi(M) \subseteq \mathfrak{a}M$. Thus by (5.44.(v)) there are an $N \geq 1$ and some $b_0, \ldots, b_{N-1} \in \mathfrak{a}$ such that $\varphi^N + b_{N-1}\varphi^{N-1} + \cdots + b_1\varphi + b_0 \mathbb{1} = 0 \in \mathrm{end}(M)$. In particular for $1_S \in M$ we have found that x is integral over $\mathfrak{a}$, as it satisfies an equation of the form

$$0_S = \left(\varphi^N + b_{N-1}\varphi^{N-1} + \cdots + b_1\varphi + b_0\mathbb{1}\right)(1_S) = x^{nN} + b_{N-1}x^{n(N-1)} + \cdots + b_1 x^n + b_0 1_S$$

□

Proof of (8.31):

(i) Consider any $x \in T = S[t_1, \ldots, t_n]$. That is there is a polynomial g in n variables over S, such that $x = g(t_1, \ldots, t_n)$. This again means is there are finitely many $b[q] \in S$ and multi-indices $\nu[q] \in \mathbb{N}^n$ such that

$$x = \sum_{q=1}^{N} b[q] t^{\nu(q)} = \sum_{q=1}^{N} \beta\big(b[q]\big) \cdot t^{\nu(q)}$$

Now for any $b[q] \in S = R[s_1, \ldots, s_m]$ there is another polynomial f_q in m variables, such that

$b[g] = f_q(s_1,\ldots,s_m)$. Again there are finitely many $a[p,q] \in R$ amd multiindices $\mu[p,q] \in \mathbb{N}^m$ such that

$$b[q] \;=\; \sum_{p=1}^{M} a[p,q]s^{\mu[p,q]} \;=\; \sum_{p=1}^{M} \alpha\big(a[p,q]\big)\cdot s^{\mu[p,q]}$$

Note that $\beta(s^{\mu[p,q]}) = \beta(s)^{\mu[p,q]}$, as β is a homomorphism of rings. Then - combining these equations - we find an expression that shows, that x can be expressed as a polynomial in the elements $\beta(s_1),\ldots,\beta(s_m)$ and $t_1,\ldots,t_n$. And as x has been arbitrary this means that $T : R$ is generated by these elements, as an R-algebra:

$$\begin{aligned} x &= \sum_{q=1}^{N} \beta\left(b[q]\right)\cdot t^{\nu(q)} \\ &= \sum_{q=1}^{N} \beta\left(\sum_{p=1}^{M} \alpha\big(a[p,q]\big)\cdot s^{\mu[p,q]}\right)\cdot t^{\nu(q)} \\ &= \sum_{q=1}^{N}\sum_{p=1}^{M} \beta\alpha\big(a[p,q]\big)\cdot \beta(s)^{\mu[p,q]}\, t^{\nu[q]} \\ &= \sum_{q=1}^{N}\sum_{p=1}^{M} a[p,q]\,\beta(s)^{\mu[p,q]}\, t^{\nu[q]} \end{aligned}$$

(ii) Consider two ring extensions $\alpha : R \to S$ and $\beta : S \to T$ such that $\beta\alpha : R \to T$ is integral. Then we will first prove, that $T : S$ is integral, too: So pick up any $x \in T$. By assumption there is some polynomial $m \in R[t]$ such that m is monic and $m(x) = 0$. Let us denote

$$\alpha(m) \;:=\; \sum_{k=0}^{\infty} \alpha\big(m[k]\big)t^k \;\in\; S[t]$$

Clearly $n := \alpha(m)$ is a monic polynomial over S. And by construction the R-algebra T uses the scalar multiplication $ax = \beta\alpha(a)\cdot x$. Likewise we have $sx = \beta(s)\cdot x$ in the S-algebra T and therefore

$$0 \;=\; m(x) \;=\; \beta\alpha(m)(x) \;=\; \beta(n)(x) \;=\; n(x)$$

Thus we have found a monic polynomial $n \in S[t]$ such that $n(x) = 0$ which means that x is integral over S. As x has been arbitrary we truly have an integral extension $T : S$.

(ii) We will now prove that (supposed that $\beta\alpha : R \to T$ is integral and β is injective) $S : R$ is integral, too. Thus consider any $s \in S$ and let $x := \beta(s)$. By assumption there is a monic polynomial $m \in R[t]$ such that $m(x) = 0$. We need to verify that $m(s) = 0$, too:

$$\begin{aligned} 0 &= m(x) \;=\; \sum_{k=0}^{\infty} \beta\alpha\big(m[k]\big)\cdot\beta(s)^k \\ &= \beta\left(\sum_{k=0}^{\infty} \alpha\big(m[k]\big)\cdot s^k\right) \;=\; \beta\big(m(s)\big) \end{aligned}$$

Now, as β is injective, this implies $m(s) = 0$ and as s has been arbitrary this means, that the whole extension $S : R$ is integral.

(ii) Conversely suppose both $\alpha : R \to S$ and $\beta : S \to T$ are integral, then we will prove that $\beta\alpha : R \to T$ is integral, too: So pick up any $x \in T$, by assumption there is a monic polynomial $n \in S[t]$ such that $n(x) = 0$. Let $d := \deg(n)$ and take $N := R[n[0], n[1], \ldots, n[d]] \subseteq S$. By construction we have $n \in N[t]$ and still $n(x) = 0$. So by (8.30.(i)) we have $[N[x] : N] < \infty$. But as N is generated by finitely many elements, that are integral over R (8.30.(v)) also tells us $[N : R] < \infty$. Therefore, due to (8.7.(iv)), we get

$$\big[N[x] : R\big] \;\leq\; \big[N[x] : N\big] \cdot \big[N : R\big] \;<\; \infty$$

That is $N[x] : R$ is finite and hence integral - by (8.30.(v)) again - such that there is some monic polynomial $m \in R[t]$ with $m(x) = 0$. Now, as x has been arbitrary this means $T : R$ is an integral extension.

(iii) If S is a finitely generated R-module, say $S = \mathrm{Lh}_R\{ s_1, \ldots, s_m \}$ and T is a finitely generated S-module, say $T = \mathrm{Lh}_S\{ t_1, \ldots, t_n \}$, then we have seen in (8.7.(i)), that $T = \mathrm{Lh}_R\{ s_i t_j \mid i \in 1 \ldots m, j \in 1 \ldots n \}$. In particular T is finitely generated as an R-module.

(iii) Conversely suppose T is a finitely generated R-module, then it is easy to see that T also is a finitely generated S-module: Say $T = \mathrm{Lh}_R\{ t_1, \ldots, t_n \}$ and consider any $x \in T$. That is $x = a_1 t_1 + \ldots a_n t_n$ for some $a_1, \ldots, a_n \in R$. By definition of the scalar multiplications on T this means $x = s_1 t_1 + \cdots + s_n t_n$, where we let $s_k := \alpha(a_k)$. That is $x \in \mathrm{Lh}_S\{ t_1, \ldots, t_n \}$ and as x was arbitrary we have found that $\{ t_1, \ldots, t_n \}$ also generates T as an S-module. In particular T is finitely generated as an S-module.

We now assume that R is a PID and that β is injective and need to show, that in this case S is a finitely generated R-module. To do this note, that $\beta(S) \subseteq T$ is an R-sub-module of T. But as T is finitely generated (as an R-module) and R is a PID, (3.104.(ii)) tells us that $\beta(S)$ is finitely generated as well. That is there are some $s_1, \ldots, s_n \in S$ such that $\beta(s_1), \ldots, \beta(s_n)$ generate $\beta(S)$ as an R-module. If now $x \in S$ is any element, then there are $a_1, \ldots a_n \in R$ such that

$$\begin{aligned}
\beta(s) \;&=\; \sum_{k=1}^{n} a_k \beta(s_k) \;=\; \sum_{k=1}^{n} \beta\alpha(a_k) \cdot \beta(s_k) \\
&=\; \beta\left(\sum_{k=1}^{n} \alpha(a_k) \cdot s_k \right) \;=\; \beta\left(\sum_{k=1}^{n} a_k s_k \right)
\end{aligned}$$

As β is injective we conclude $s = a_1 s_1 + \cdots + a_n s_n$. And as this is true for any $x \in S$, we see that $\{ s_1, \ldots, s_n \}$ generates S as an R module, that is $S : R$ is a finite ring extension.

□

Proof of (8.69):

(i) If $\ell(\mathcal{P}) = \mathrm{kdim}(R)$, then in particular $\mathrm{kdim}(R) < \infty$. Suppose $\mathcal{P}$ was not maximal, then there was some $\mathcal{P}' \in \mathrm{CPI}(R)$ with $\mathcal{P} < \mathcal{P}'$ and in particular $\ell(\mathcal{P}) < \ell(\mathcal{P}')$. But $\mathrm{kdim}(R) < \ell(\mathcal{P}')$ is absurd, such that $\mathcal{P}$ has to be maximal.

(ii) Consider any CPI $\mathfrak{p}_0 \subset \ldots \subset \mathfrak{p}_r$ in R. Then we pull this chain back into S, that is we define the

following ideals in S

$$\mathfrak{q}_i \;:=\; \varphi^{-1}(\mathfrak{p}_i) \;=\; \{\, x \in S \mid \varphi(x) \in \mathfrak{p}_i \,\}$$

These are prime ideals: If $xy \in \mathfrak{q}_i$ then $\varphi(x)\varphi(y) = \varphi(xy) \in \mathfrak{p}_i$ and as $\mathfrak{p}_i$ is prime we get $\varphi(x) \in \mathfrak{p}_i$ or $\varphi(y) \in \mathfrak{p}_i$ which again is $x \in \mathfrak{q}_i$ or $y \in \mathfrak{q}_i$. From the construction it also is clear that the $\mathfrak{q}_i$ form an ascending chain

$$\mathfrak{q}_0 \;\subseteq\; \mathfrak{q}_1 \;\subseteq\; \ldots \;\subseteq\; \mathfrak{q}_r$$

Assume we had $\mathfrak{q}_{i-1} = \mathfrak{q}_i$ for some $i \in 1 \ldots r$. Then also $\varphi(\mathfrak{q}_{i-1}) = \varphi(\mathfrak{q}_i)$. But as φ is surjective we have $\varphi(\mathfrak{q}_i) = \varphi(\varphi^{-1}(\mathfrak{p}_i)) = \mathfrak{p}_i$ for any subset $\mathfrak{p}_i \subseteq R$, according to (0.10). That is we would have $\mathfrak{p}_{i-1} = \mathfrak{p}_i$, which is untrue. Thus $\mathfrak{q}_{i-1} \subset \mathfrak{q}_i$ which means that we have found a CPI in S of length r as well. So there are two cases: (1) If $r = \operatorname{kdim}(R) < \infty$ then we find a CPI in S of length r and hence $\operatorname{kdim}(R) = r \leq \operatorname{kdim}(S)$. (2) If $\operatorname{kdim}(R) = \infty$ then there are CPI in R of undounded length r. Then we conclude, that S features CPI of unbounded length, too and hence $\operatorname{kdim}(S) = \infty = \operatorname{kdim}(R)$. In both cases we have $\operatorname{kdim}(R) \leq \operatorname{kdim}(S)$, as claimed.

(iii) Consider any prime ideal $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ of $\operatorname{height}(\mathfrak{p}) = 0$. We want to prove, that $\mathfrak{p}$ is minimal. So pick up any $\mathfrak{p}' \trianglelefteq_{\mathrm{i}} R$ such that $\mathfrak{p}' \subseteq \mathfrak{p}$. Suppose $\mathfrak{p}' \neq \mathfrak{p}$ then we had a CPI $(\mathfrak{p}', \mathfrak{p}) \in \operatorname{CPI}(R)$ of length 1. But as $\operatorname{height}(\mathfrak{p}) = 0$ no such chain exists and therefore $\mathfrak{p}' = \mathfrak{p}$.

Conversely consider any $\mathfrak{p} \in \operatorname{Smin}(R)$ and any CPI $(\mathfrak{p}_0, \ldots, \mathfrak{p}_r)$ in R with $\mathfrak{p}_r = \mathfrak{p}$. In particular $\mathfrak{p}_0 \subseteq \mathfrak{p}$. As $\mathfrak{p}$ is minimal, this implies $\mathfrak{p}_0 = \mathfrak{p} = \mathfrak{p}_r$ which means $r = 0$. As this is true for any $\operatorname{CPI}^{\mathfrak{p}}(R)$ we conclude $\operatorname{height}(\mathfrak{p}) = 0$. means

(iv) If $(\mathfrak{p}_0, \ldots, \mathfrak{p}_r)$ is a chain of prime ideals of R, then by (2.19.(iii)) we find a chain of pirime ideals $(\mathfrak{p}_0/\operatorname{NIL}(R), \ldots, \mathfrak{p}_r/\operatorname{NIL}(R))$ of $R/\operatorname{NIL}(R)$ and vice versa, as the spectra of R and $R/\operatorname{NIL}(R)$ are in one-to-one correspondence. But as this correspondence obviously preserves inclusion and length we have both $\operatorname{kdim}(R) \leq \operatorname{kdim}(R/\operatorname{NIL}(R))$ and $\operatorname{kdim}(R/\operatorname{NIL}(R)) \leq \operatorname{kdim}(R)$.

(v) As $\operatorname{Smax}(R) \subseteq \operatorname{Spec}(R) \subseteq \operatorname{Ideal}(R)$ the supremum of all the $\operatorname{height}(\mathfrak{m})$ where $\mathfrak{m} \in \operatorname{Smax}(R)$ yields the lowest number. Hence it suffices to find a maximal ideal $\mathfrak{m}$ such that for any ideal $\mathfrak{a}$ we have $\operatorname{height}(\mathfrak{a}) \leq \operatorname{height}(\mathfrak{m})$.

If $\operatorname{kdim}(R) < \infty$, then we pick up a CPI $(\mathfrak{q}_0, \ldots, \mathfrak{q}_n)$ with $n = \operatorname{kdim}(R)$. Now by (i) we have $\mathfrak{m} := \mathfrak{q}_n \in \operatorname{Smax}(R)$. If now $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ is any proper ideal and $\mathfrak{p} \in \operatorname{Spec}(R)$ is any prime ideal with $\mathfrak{a} \subseteq \mathfrak{p}$, then we take a look at a CPI $(\mathfrak{p}_0, \ldots, \mathfrak{p}_m)$ with $\mathfrak{p}_m = \mathfrak{p}$ and $m = \operatorname{height}(\mathfrak{p})$. As $(\mathfrak{p}_0, \ldots, \mathfrak{p}_m)$ is a CPI in R we have $\operatorname{height}(\mathfrak{p}) = m \leq \operatorname{kdim}(R) = n = \operatorname{height}(\mathfrak{m})$. This means $\operatorname{height}(\mathfrak{a}) \leq \operatorname{height}(\mathfrak{m})$, as needed. And for $\mathfrak{a} = R$ this inequality is satisfied trivially, as we defined $\operatorname{height}(R) = -1 \leq 0 \leq n = \operatorname{height}(\mathfrak{m})$.

If $\operatorname{kdim}(R) = \infty$ there are CPIs of unbounded length. If the largest ideal of these is not maximal already, we can even append such a chain by a maximal ideal containing it. Hence R also features CPIs of unbounded length ending in maximal ideals and hence the supremum of the length of these chains is infinite, too. Again all suprema are equal - in this case equal to infinity.

(vi) Pick up a CPI $(\mathfrak{p}_0, \ldots, \mathfrak{p}_m)$ with $\mathfrak{p}_m = \mathfrak{p}$, as $\mathfrak{p} \subseteq \mathfrak{q}$, by assumption, this gives rise to a CPI $(\mathfrak{p}_0, \ldots, \mathfrak{p}_m, \mathfrak{q})$ of length $m+1$. Thus if $\mathfrak{p}$ had infinite height, then we could find CPI of unbounded

length ending in $\mathfrak{p}$ and therefore also even longer CPI, ending in $\mathfrak{q}$ such that $\text{height}(\mathfrak{p}) = \infty$ implies $\text{height}(\mathfrak{q}) = \infty$, too. So by assumption $\text{height}(\mathfrak{q}) < \infty$ we also have $\text{height}(\mathfrak{p}) < \infty$.

Therefore we may choose a CPI, as above, with $m = \text{height}(\mathfrak{p})$. As this can be appended to a CPI of length $m+1$ ending in $\mathfrak{q}$, this ideal has height $m+1$ at least. Altogether we conclude

$$\text{height}(\mathfrak{p}) \;=\; m \;<\; m+1 \;\leq\; \text{height}(\mathfrak{q})$$

(vii) Suppose $\mathfrak{p}$ was *not* minimal over $\mathfrak{a}$, that is there is some prime ideal $\mathfrak{p}' \in \text{Spec}(R)$, such that $\mathfrak{a} \subseteq \mathfrak{p}' \subset \mathfrak{p}$. In particular we have $\text{height}(\mathfrak{p}') < \text{height}(\mathfrak{p})$ by (vi). But as $\mathfrak{a} \subseteq \mathfrak{p}'$ we also have $\text{height}(\mathfrak{a}) \leq \text{height}(\mathfrak{p}')$ and together that is

$$\text{height}(\mathfrak{p}) \;=\; \text{height}(\mathfrak{a}) \;\leq\; \text{height}(\mathfrak{p}') \;<\; \text{height}(\mathfrak{p})$$

a contradiction. Thus there is no such $\mathfrak{p}'$ and hence $\mathfrak{p}$ is minimal over $\mathfrak{a}$. It remains to verify the following identity of the height of $\mathfrak{a}$

$$\text{height}(\mathfrak{a}) \;\;=\;\; \min\{\, \text{height}(\mathfrak{p}) \mid \mathfrak{p} \in \mathbb{V}(\mathfrak{a})_* \,\}$$

As $\mathfrak{a} \neq R$ is proper there is a maximal ideal $\mathfrak{m}$ of R containing $\mathfrak{a} \subseteq \mathfrak{m}$, by (2.4.(ii)). Now by (2.18.(iv)) there is a prime ideal $\mathfrak{p}$ of R minimal over $\mathfrak{a}$, with $\mathfrak{a} \subseteq \mathfrak{p} \subseteq \mathfrak{m}$ and in particular $\mathfrak{p} \in \mathbb{V}(\mathfrak{a})_*$. Thus the set, we take the minimum over, is non-empty and hence the minimum is well-defined.

Recall that $\text{height}(\mathfrak{a}) = \min\{\, \text{height}(\mathfrak{p}) \mid \mathfrak{p} \in \mathbb{V}(\mathfrak{a}) \,\}$, by definition. As $\mathbb{V}(\mathfrak{a})_* \subseteq \mathbb{V}(\mathfrak{a})$ is a subset, we conclude that $\text{height}(\mathfrak{a})$ cannot exceed the minimum above. Conversely let $\mathfrak{p} \in \mathbb{V}(\mathfrak{a})$ such that $\text{height}(\mathfrak{p})$ is minimal, that is $\text{height}(\mathfrak{p}) = \text{height}(\mathfrak{a})$. Then we have argued obove, that $\mathfrak{p}$ is minimal over $\mathfrak{a}$ that is $\mathfrak{p} \in \mathbb{V}(\mathfrak{a})_*$. Thus we find that the minimal height is assumed by an element of the subset $\mathbb{V}(\mathfrak{a})_*$ and hence the minima over $\mathbb{V}(\mathfrak{a})$ and $\mathbb{V}(\mathfrak{a})_*$ are equal.

(ix) By (8.65.(ii)) there is a one-to-one correspondence between the prime ideals of $R_\mathfrak{p}$ and the prime ideals of R, contained in $\mathfrak{p}$. Thus any CPI $(\mathfrak{u}_0, \ldots, \mathfrak{u}_m)$ of $R_\mathfrak{p}$ is of the form $\mathfrak{u}_k = \mathfrak{p}_k R_\mathfrak{p}$ for a CPI $(\mathfrak{p}_0, \ldots, \mathfrak{p}_m)$ of R with $\mathfrak{p}_m \subseteq \mathfrak{p}$. If one has CPIs of length m, then so does the other. So if $(\mathfrak{p}_0, \ldots, \mathfrak{p}_m)$ is the CPI of R with $\mathfrak{p}_m = \mathfrak{p}$ and $m = \text{height}(\mathfrak{p})$ then we can conclude $\text{kdim}(R_\mathfrak{p}) \geq \text{height}(\mathfrak{p})$, as we get the CPI $(\mathfrak{p}_0 R_\mathfrak{p}, \ldots, \mathfrak{p}_m R_\mathfrak{p})$ of $R_\mathfrak{p}$. But conversely if $(\mathfrak{u}_0, \ldots, \mathfrak{u}_m)$ is the CPI of $R_\mathfrak{p}$ with $\text{kdim}(R_\mathfrak{p}) = m$ then this corresponds to some CPI $(\mathfrak{p}_0, \ldots, \mathfrak{p}_m)$ of R with $\mathfrak{p}_m \subseteq \mathfrak{p}$ and hence $\text{height}(\mathfrak{p}) \geq \text{kdim}(R_\mathfrak{p})$, as well. And if one has infinite dimension, there are arbitrarily long CPI, so the other has infinite dimension, as well.

(x) As R is finite-dimensional, so is $R/\mathfrak{a}$, as any CPI $(\overline{\mathfrak{q}}_0, \ldots, \overline{\mathfrak{q}}_s)$ in $R/\mathfrak{a}$ is inherited from a CPI of R, by the correspondence theorem of ideals (1.71). That is any $\overline{\mathfrak{q}}_j$ is of the form $\overline{\mathfrak{q}}_j = \mathfrak{q}_j/\mathfrak{a}$ for some prime ideal $\mathfrak{q}_j \in \text{Spec}(R)$ with $\mathfrak{a} \subseteq \mathfrak{q}_j$. So pick up such a CPI with $s = \text{kdim}(R/\mathfrak{a})$. As $\mathfrak{a} \subseteq \mathfrak{q}_0$ we have $\text{height}(\mathfrak{a}) \leq \text{height}(\mathfrak{q}_0)$. Thereby $\text{height}(\mathfrak{p}_0)$ is finite, as R was assumed to be finite-dimensional and hence *any* CPI in R is of finite length. Thus we may also pick up a CPI $(\mathfrak{p}_0, \ldots, \mathfrak{p}_r)$ of R such that $\mathfrak{p}_r = \mathfrak{q}_0$ and $r = \text{height}(\mathfrak{q}_0)$. Let us attach these chains in $\mathfrak{p}_r = \mathfrak{q}_0$:

$$(\mathfrak{p}_0, \ldots, \mathfrak{p}_r = \mathfrak{q}_0, \mathfrak{q}_1, \ldots, \mathfrak{q}_s) \;\;\in\;\; \text{CPI}(R)$$

This is a chain of length $r+s$ in R and thereby we have $\operatorname{kdim}(R) \geq r+s$. But as $r = \operatorname{height}(\mathfrak{q}_0)$ and $s = \operatorname{kdim}(R/\mathfrak{a})$ by construction, this means $\operatorname{kdim}(R) \geq \operatorname{height}(\mathfrak{q}_0) + \operatorname{kdim}(R/\mathfrak{a})$. But we also have $\operatorname{height}(\mathfrak{q}_0) \geq \operatorname{height}(\mathfrak{a})$ and thereby the claim

$$\operatorname{kdim}(R) \;\geq\; \operatorname{height}(\mathfrak{q}_0) + \operatorname{height}\left(R\Big/\mathfrak{a}\right) \;\geq\; \operatorname{height}(\mathfrak{a}) + \operatorname{height}\left(R\Big/\mathfrak{a}\right)$$

(xi) As $\operatorname{height}(\mathfrak{q}) < \infty$ is finite, so is $\operatorname{height}(\mathfrak{q}/\mathfrak{p})$. So let $\mathfrak{q}_0/\mathfrak{p} \subset \ldots \subset \mathfrak{q}_s/\mathfrak{p}$ be a CPI in $R/\mathfrak{p}$ such that $\mathfrak{q}_s/\mathfrak{p} = \mathfrak{q}/\mathfrak{p}$ and $s = \operatorname{height}(\mathfrak{q}/\mathfrak{p})$. Note that this is $\mathfrak{q}_s = \mathfrak{q}$. Now suppose we had $\mathfrak{q}_0 \neq \mathfrak{p}$, as $\mathfrak{p} \subseteq \mathfrak{q}_0$ by correspondence, the non-identity means $0 \subset \mathfrak{q}_0/\mathfrak{p}$. But as $\mathfrak{p}$ is a prime ideal $0 \in \operatorname{Spec}(R/\mathfrak{p})$ is a prime ideal. Thus $0 \subset \mathfrak{q}_0/\mathfrak{p} \subset \ldots \subset \mathfrak{q}_s/\mathfrak{p}$ would be a even longer chain, contradicting the maximality of $s = \operatorname{height}(\mathfrak{q}/\mathfrak{p})$. Thus we conclude $\mathfrak{q}_0 = \mathfrak{p}$, as well. Also as $\mathfrak{p} \subseteq \mathfrak{q}$ the height of $\mathfrak{p}$ is finite, too and hence we may pick up another CPI $\mathfrak{p}_0 \subset \ldots \subset \mathfrak{p}_r$ in R with $\mathfrak{p}_r = \mathfrak{p}$ and $r = \operatorname{height}(\mathfrak{p})$. But then we can compose these chains to a CPI of length $r+s$ in R

$$\mathfrak{p}_0 \;\subseteq\; \ldots \;\subset\; \mathfrak{p}_r = \mathfrak{p} = \mathfrak{q}_0 \;\subset\; \mathfrak{q}_1 \;\subset\; \ldots \;\subset\; \mathfrak{q}_s = \mathfrak{q}$$

In particular $\operatorname{height}(\mathfrak{q}) \geq r+s$ such that $\operatorname{height}(\mathfrak{q}/\mathfrak{p}) = s \leq \operatorname{height}(\mathfrak{q}) - r = \operatorname{height}(\mathfrak{q}) - \operatorname{height}(\mathfrak{p})$.

(viii) Let us first prove the statements for $n = \operatorname{kdim}(R)$: (2) Let $k \in 1\ldots n$ and consider any prime ideal $\mathfrak{p}'$ of R such that $\mathfrak{p}_{k-1} \subseteq \mathfrak{p}' \subseteq \mathfrak{p}_k$. If we even had $\mathfrak{p}_{k-1} \subset \mathfrak{p}' \subset \mathfrak{p}_k$ then we could build up a CPI $(\mathfrak{p}_0, \ldots, \mathfrak{p}_{k-1}, \mathfrak{p}', \mathfrak{p}_k, \ldots, \mathfrak{p}_n)$ of length $n+1$. But such a chain does not exist as there are no chains of length greater $\operatorname{kdim}(R) = n$. Thus we must either have $\mathfrak{p}' = \mathfrak{p}_{k-1}$ or $\mathfrak{p}' = \mathfrak{p}_k$ and this is the claim $\mathfrak{p}_{k-1} \subset_* \mathfrak{p}_k$, that $\mathfrak{p}_{k-1}$ lies directly under $\mathfrak{p}_k$.

(3) First of all we have $n \leq \operatorname{height}(\mathfrak{p}_n)$, as there is a CPI of length n that ends in $\mathfrak{p}_n$ - namely $(\mathfrak{p}_0, \ldots, \mathfrak{p}_n)$ itself. On the other hand $\operatorname{height}(\mathfrak{p}_n) \leq \operatorname{kdim}(R) = n$ is generally true. Thus we conclude $\operatorname{height}(\mathfrak{p}_n) = n$. Let us now abbreviate $h(k) := \operatorname{height}(\mathfrak{p}_k)$, then we have just seen $h(n) = n$. Also by (vi) we have $h(k-1) = \operatorname{height}(\mathfrak{p}_{k-1}) < \operatorname{height}(\mathfrak{p}_k) = h(k)$ for any $k \in 1\ldots n$, as $\mathfrak{p}_{k-1} \subset \mathfrak{p}_k$ and we deal with a CPI. That is $0 \leq h(0) < \cdots < h(n) = n$. In particular $h(k) \leq n$ for any $k \in 0\ldots n$ and thereby we have found a map

$$h \;:\; 0\ldots n \hookrightarrow 0\ldots n \;:\; k \mapsto \operatorname{height}(\mathfrak{p}_k)$$

This map is injective, as it is strictly monotonous. Well, in the finite set $0\ldots n$ there is one map and one map only, that can do this and this is the identity $h(k) = k$. (1) In particular we have $\operatorname{height}(\mathfrak{p}_0) = 0$ and this already means $\mathfrak{p}_0 \in \operatorname{Smin}(R)$, by (iii). As $\mathfrak{p}_n$ is a prime ideal, it is proper $\mathfrak{p}_n \neq R$ and therefore by (2.4.(ii)) there is a maximal ideal $\mathfrak{m} \in \operatorname{Smax}(R)$ containing it $\mathfrak{p}_n \subseteq \mathfrak{m}$. Suppose we had $\mathfrak{p}_n \neq \mathfrak{m}$ then $\mathfrak{p}_n \subset \mathfrak{m}$ and thereby we had another CPI $(\mathfrak{p}_0, \ldots, \mathfrak{p}_n, \mathfrak{m})$ of length $n+1 > n = \operatorname{kdim}(R)$. As this cannot be, we have $\mathfrak{p}_n = \mathfrak{m}$ and thereby $\mathfrak{p}_n \in \operatorname{Smax}(R)$.

Now consider the case of a CPI $(\mathfrak{p}_0, \ldots, \mathfrak{p}_r)$ of length $r = \operatorname{height}(\mathfrak{p}_r)$ and abbreviate $\mathfrak{p} := \mathfrak{p}_r$. Then we take to the localisation $R_\mathfrak{p}$ of R in $\mathfrak{p}$. By CPI-correspondence (8.65.(ii)) the transferred chain $(\mathfrak{p}_0 R_\mathfrak{p}, \ldots, \mathfrak{p}_r R_\mathfrak{p})$ in $R_\mathfrak{p}$ is of length

$$r \;=\; \operatorname{height}(\mathfrak{p}) \;=\; \operatorname{kdim}\big(R_\mathfrak{p}\big)$$

according to (ix). Thus by the above it satisfies properties (1), (2) and (3) of a CPI whose length equals the Krull-dimension. Returning to $(\mathfrak{p}_0,\ldots,\mathfrak{p}_r)$ with CPI-correspondence again, we retain properties (2), (3) and $\mathfrak{p}_0 \in \mathrm{Smin}(R)$. This is the shortcut, bu of course it is possible to redo the above arguments with the CPI $(\mathfrak{p}_0,\ldots,\mathfrak{p}_r)$ again.

(xii) Consider $\mathfrak{p} \in \mathrm{Spec}(R)$ with $\mathfrak{p} \subset_* \mathfrak{q}$, in particular we have $\mathfrak{p} \subset \mathfrak{q}$ and therefore $\mathrm{height}(\mathfrak{p}) < \mathrm{height}(\mathfrak{q})$ according to (vi). That is $1+\mathrm{height}(\mathfrak{p}) \leq \mathrm{height}(\mathfrak{q})$ and as this is true for any $\mathfrak{p}$ we have found that the supremum cannot exceed $\mathrm{height}(\mathfrak{q})$.

Conversely, as $\mathfrak{q}$ is of finite height we may pick up a CPI $(\mathfrak{q}_0,\ldots,\mathfrak{q}_s)$ such that $\mathfrak{q}_s = \mathfrak{q}$ and $s = \mathrm{height}(\mathfrak{q})$. Clearly $\mathrm{height}(\mathfrak{q}_{s-1}) \geq s-1$ as it has the $s-1$ prime ideals $\mathfrak{q}_k$ for $k \in 0\ldots s-1$ underneath. Suppose there was an even longer CPI ending in $\mathfrak{q}_{s-1}$ say $(\mathfrak{r}_0,\ldots,\mathfrak{r}_t)$ with $\mathfrak{r}_t = \mathfrak{q}_{s-1}$ and $t > s-1$. Then we could build up the CPI $(\mathfrak{r}_0,\ldots,\mathfrak{r}_t,\mathfrak{q})$ and have $t+1 > s = \mathrm{height}(\mathfrak{q})$ in contradiction to s being the maximal length under $\mathfrak{q}$. Thus we have $\mathrm{height}(\mathfrak{q}_{s-1}) = s-1$.

Now suppose there was some $\mathfrak{q}' \in \mathrm{Spec}(R)$ with $\mathfrak{q}_{s-1} \subset \mathfrak{q}' \subset \mathfrak{q}$. Then we would find a CPI $(\mathfrak{q}_0,\ldots,\mathfrak{q}_{s-1},\mathfrak{q}',\mathfrak{q})$ of length $s+1$ ending in $\mathfrak{q}$. Again this does not exist, as $s = \mathrm{height}(\mathfrak{q})$ is the limit. Thus we have $\mathfrak{q}' = \mathfrak{q}_{s-1}$ or $\mathfrak{q}' = \mathfrak{q}$ and this means $\mathfrak{q}_{s-1} \subset_* \mathfrak{q}$ lies directly under $\mathfrak{q}$. In particular the set inside the supremum is non-empty. But then we have found a $\mathfrak{p} := \mathfrak{q}_{s-1}$ satisfying $\mathfrak{p} \subset_* \mathfrak{q}$ and $\mathrm{height}(\mathfrak{q}) = 1+\mathrm{height}(\mathfrak{p})$ and hence the height of $\mathfrak{q}$ cannot exceed the supremum, as well. Thus both have to be equal.

(xiii) Let us abbreviate the quotient ring by $Q := R/\mathfrak{a}$ and the prime ideal $\overline{\mathfrak{p}} := \mathfrak{p}/\mathfrak{a}$ of Q, then we have to verify the claim $\mathrm{height}(\overline{\mathfrak{p}}) < \mathrm{height}(\mathfrak{p})$: So pick up any CPI $(\mathfrak{q}_0,\ldots,\mathfrak{q}_s)$ in Q ending in $\mathfrak{q}_s = \overline{\mathfrak{p}}$. By the correspondence theorem of ideals (1.71) these $\mathfrak{q}_k$ are of the form $\mathfrak{q}_k = \mathfrak{p}_k/\mathfrak{a}$ for some $\mathfrak{p}_k \in \mathrm{Spec}(R)$ with $\mathfrak{a} \subseteq \mathfrak{p}_k$. That is we have a CPI $(\mathfrak{p}_0,\ldots,\mathfrak{p}_s)$ of length s in R with $\mathfrak{p}_s = \mathfrak{p}$. Now pick up a prime ideal $0 \subseteq \mathfrak{p}_* \subseteq \mathfrak{p}_0$ that is minimal over 0, by (2.18.(iv)). As this is a minimal prime ideal in R we have $\mathfrak{p}_* \subseteq \mathrm{zD}(R)$ by (2.19.(ii)). But by assumption we have $a \in \mathrm{nzD}(R)$ such that $a \notin \mathfrak{p}_*$ whereas $a \in \mathfrak{a} \subseteq \mathfrak{p}_0$. Thus $\mathfrak{p}_* \subset \mathfrak{p}_0$ is strictly contained and thereby we have found a CPI in R of length $s+1$

$$\mathfrak{p}_* \subset \mathfrak{p}_0 \subset \ldots \subset \mathfrak{p}_s = \mathfrak{p}$$

ending in $\mathfrak{p}$. That is $\mathrm{height}(\mathfrak{p}) \geq s+1 > s$. As this is true for any CPI $(\mathfrak{q}_0,\ldots,\mathfrak{q}_s)$ in Q ending in $\overline{\mathfrak{p}}$ we have $\mathrm{height}(\overline{\mathfrak{p}}) < \mathrm{height}(\mathfrak{p})$. If $\overline{\mathfrak{p}}$ is of infinite height, then so is $\mathrm{height}(\mathfrak{p})$.

□

Proof of (8.72):

(i) If $\mathfrak{q}$ is a prime ideal of S, then $\mathfrak{q} \cap R$ is a prime ideal of R, according to (2.17) and it is clear, that $\mathfrak{q}_{i-1} \subseteq \mathfrak{q}_i$ implies $\mathfrak{q}_{i-1} \cap R = \alpha^{-1}(\mathfrak{q}_{i-1}) \subseteq \alpha^{-1}(\mathfrak{q}_i) = \mathfrak{q}_i \cap R$. Now suppose $\mathfrak{q}_{i-1} \cap R = \mathfrak{q}_i \cap R$, as $\mathfrak{q}_{i-1} \subseteq \mathfrak{q}_i$ we get $\mathfrak{q}_{i-1} = \mathfrak{q}_i$ by (8.32.(iii)). But this is untrue, such that $\mathfrak{q}_{i-1} \cap R \subset \mathfrak{q}_i$ for any $i \in 1\ldots r$ such that the pull-back truly is a CPI in R again.

(ii) By induction it is clear, that we only need to take the first step, that is we regard $\mathfrak{p}_0 \subset \mathfrak{p}_1 \in \mathrm{Spec}(R)$ and start with some $\mathfrak{q}_0 \in \mathrm{Spec}(S)$ such that $\mathfrak{q}_0 \cap R = \mathfrak{p}_0$. Then by (8.29.(iv)) $S/\mathfrak{q}_0 : R/\mathfrak{p}_0$ is an integral extension, as well. By the correspondence theorem of ideals $\mathfrak{p}_1/\mathfrak{p}_0$ is a prime ideal

of $R/\mathfrak{p}_0$ and as $\mathfrak{p}_0 \subset \mathfrak{p}_1$ this ideal is non-zero $\mathfrak{p}_1/\mathfrak{p}_0 \neq 0$. By the lying-over theorem (8.32.(i)) there is a prime ideal $\mathfrak{q}_1/\mathfrak{q}_0 \trianglelefteq_{\mathrm{i}} S/\mathfrak{q}_0$ such that

$$\mathfrak{q}_1 \Big/ \mathfrak{q}_0 \cap R \Big/ \mathfrak{p}_0 \;=\; \mathfrak{p}_1 \Big/ \mathfrak{p}_0$$

By the correspondence theorem of ideals again $\mathfrak{q}_1 \in \operatorname{Spec}(S)$ is a prime ideal, as well. It remains to prove $\mathfrak{q}_1 \cap R = \mathfrak{p}_0$. So let us take a closer look at at the identity of the pull-back of $\mathfrak{q}_1/\mathfrak{q}_0$: If $\alpha : R \to S$ is the structural homomorphism, then the induced structural homomorphism $\overline{\alpha}$ maps $a + \mathfrak{p}_0 \mapsto \alpha(a) + \mathfrak{q}_0$ and therefore

$$\begin{aligned} \mathfrak{p}_1 \Big/ \mathfrak{p}_0 &= \mathfrak{q}_1 \Big/ \mathfrak{q}_0 \cap R \Big/ \mathfrak{p}_0 \\ &= \left\{ a + \mathfrak{p}_0 \mid \overline{\alpha}(a + \mathfrak{p}_0) \in \mathfrak{q}_1 \Big/ \mathfrak{q}_0 \right\} \\ &= \left\{ a + \mathfrak{p}_0 \mid \alpha(a) + \mathfrak{q}_0 \in \mathfrak{q}_1 \Big/ \mathfrak{q}_0 \right\} \end{aligned}$$

We also have $\mathfrak{p}_0 = \mathfrak{q}_0 \cap R = \{ a \mid \alpha(a) \in \mathfrak{q}_0 \}$. With these two properties we are able to prove $\mathfrak{p}_1 = \mathfrak{q}_1 \cap R = \{ a \mid \alpha(a) \in \mathfrak{q}_1 \}$. So if we start with $a \in \mathfrak{p}_1$ then $a + \mathfrak{p}_0 \in \mathfrak{p}_1/\mathfrak{p}_0$ and hence $\alpha(a) + \mathfrak{p}_0 \in \mathfrak{q}_1/\mathfrak{p}_0$. But this is $\alpha(a) \in \mathfrak{q}_1$ and therefore $a \in \mathfrak{q}_1 \cap R$. Conversely $a \in \mathfrak{q}_1 \cap R$ means $\alpha(a) \in \mathfrak{q}_1$ and hence $\alpha(a) + \mathfrak{q}_0 \in \mathfrak{q}_1/\mathfrak{q}_0$. By the identity above this means $a + \mathfrak{p}_0 \in \mathfrak{p}_1/\mathfrak{p}_0$ and hence $a \in \mathfrak{p}_1$. Thus we have the equality $\mathfrak{p}_1 = \mathfrak{q}_0 \cap R$.

(iii) By induction it is clear, that we only need to take the first step, that is we regard $\mathfrak{p}_0 \subset \mathfrak{p}_1 \in \operatorname{Spec}(R)$ and start with some $\mathfrak{q}_1 \in \operatorname{Spec}(S)$ such that $\mathfrak{q}_1 \cap R = \mathfrak{p}_1$. The proof however will require several steps: In the first step we will require S to be an *integral domain*. Then we localize S in $\mathfrak{q}_1$ that is we look at $S_{\mathfrak{q}_1}$. As S is an integral domain $\kappa : S \to S_{\mathfrak{q}_1} : x \mapsto x/1$ is injective. Let $\alpha : R \hookrightarrow S : a \mapsto a1_S$ be the structural homomorphism again, as S is R-torsion-free, α is injective, too. Now $S_{\mathfrak{q}_1} : R$ becomes an R-algebra under the structural homomorphism $\alpha_1 := \kappa\alpha$. As both α and κ are injective, so is α_1. That is

$$\alpha_1 \;:\; R \hookrightarrow S_{\mathfrak{q}_1} \;:\; a \mapsto \frac{\alpha(a)}{1}$$

- For any ideal $\mathfrak{p}_0$ we have $\mathfrak{p}_0 \subseteq \mathfrak{p}_0 S_{\mathfrak{q}_1} \cap R$ due to (8.15). We now claim, that the converse inclusion is true, as well. That is we set out on a lengthy journey to prove

$$\mathfrak{p}_0 S_{\mathfrak{q}_1} \cap R \quad\subseteq\quad \mathfrak{p}_0$$

Consider any $a \in \mathfrak{p}_0 S_{\mathfrak{q}_1} \cap R$, then we need to show $a \in \mathfrak{p}_0$. If $a = 0$, then $a \in \mathfrak{p}_0$ is granted, such that we only have to regard the case $a \neq 0$. By assumption a satisfies $\alpha_1(a) \in \mathfrak{p}_0 S_{\mathfrak{q}_1}$. That is there are some $s_i \in S$ and $u_i \in S \setminus \mathfrak{q}_1$ and $p_i \in \mathfrak{p}_0$ such that we have an identity of the form

$$\frac{\alpha(a)}{1} \;=\; \frac{s_1}{u_1} p_1 + \cdots + \frac{s_k}{u_k} p_k$$

By taking $u := u_1 \dots u_k \in S \setminus \mathfrak{q}_1$ and as always $\widehat{u_i} := u/u_i \in R$ we find that $\alpha(a)/1 = y/u$ for

$$y \;:=\; \sum_{i=1}^{k} \widehat{u_i} s_i p_i \;\in\; \mathfrak{p}_0 S$$

By assumption $S : R$ is integral, that is $S = \overline{R} := \mathrm{int}(S : R)$ and hence y is integral over $\mathfrak{p}_0$ as we know from (8.30.(ix)). That is it satisfies an equation $f \in R[t]$ of the form

$$f(y) \;:=\; y^n + f[n-1]y^{n-1} + \cdots + f[1]y + f[0] \;=\; 0$$

where $f[i] \in \mathfrak{p}_0$. On the other hand, as R is a normal domain, $y \in S$ has a minimal polynomial $m_y \in R[t]$, according to (8.37). And therefore we get $f = g m_y$ for some $g \in R[t]$. Now take a look at $\varrho : R \twoheadrightarrow R/\mathfrak{p}_0 : a \mapsto a + \mathfrak{p}_0$ which induces a homomorphism on the polynomial rings

$$\overline{\varrho} \;:\; R[t] \twoheadrightarrow {}^{R}\Big/_{\mathfrak{p}_0}[t] \;:\; f \mapsto \overline{f} := \sum_{k \in \mathbb{N}} \big(f[k] + \mathfrak{p}_0\big) t^k$$

Inserting $f = g m_y$ we get $t^n = \overline{f} = \overline{g}\,\overline{m}_y$ and as $R/\mathfrak{p}_0$ is an integral domain this means $\overline{m}_y = t^r$ and $\overline{g} = t^{n-r}$ for some $r \in 0 \dots n$. That is m_y is of the form

$$m_y \;=\; t^r + m_y[r-1]t^{r-1} + \cdots + m_y[1]t + m_y[0]$$

for some $m_y[i] \in \mathfrak{p}_0$. Let $F := \mathrm{quot}(S)$, which is possible, as we assumed S to be an integral domain, for now, and consider $S_{\mathfrak{q}_0} \subseteq F$ as a subset, canonically. Then $\alpha(a)/1 = y/u$ turns into the equation $1/\alpha(a) = u/y$ in F. Note that $\alpha(a) \neq 0$, as S is R-torsion free and hence $y \neq 0$. And thereby we get

$$\begin{aligned}
0 \;&=\; \frac{1}{\alpha(a)^r} m_y(y) \;=\; \frac{u^r}{y^r}\left(y^r + \sum_{k=0}^{r-1} m_y[k] y^k\right) \\
&=\; u^r + \sum_{k=0}^{r-1} m_y[k] \frac{u^r}{y^r} y^k \;=\; u^r + \sum_{k=0}^{r-1} m_y[k] \frac{u^{r-k}}{y^{r-k}} u^k \\
&=\; u^r + \sum_{k=0}^{r-1} m_y[k] \frac{1}{\alpha(a)^{r-k}} u^k \;=\; u^r + \sum_{k=0}^{r-1} \frac{\alpha(m_y[k])}{\alpha(a)^{r-k}} u^k
\end{aligned}$$

Note that for any $a \in R$ and $x \in S$ we have $ax = \alpha(a) \cdot x$ by definition of a ring extension. The scalar multiplication with $m_y[k]$ turned into a multiplication with $\alpha(m_y[k]) = \alpha(m_y[k])/1$ in F. If we take $E := \mathrm{quot}(R)$ then $E \hookrightarrow F$ by $a/b \mapsto \alpha(a)/\alpha(b)$, as $\alpha(a)/\alpha(b) = \alpha(c)/\alpha(d)$ implies $\alpha(ad) = \alpha(bc)$ which in turn yields $ad = bc$ [as α is injective] such that $a/b = c/d$ again. In this sense we regard E as a subset of F. Then $\alpha(m_y[k])/\alpha(a)^{r-k} = m_y[k]/a^{r-k} \in E$ and thereby we have found a monic polynomial

$$m_u \;:=\; \frac{1}{a^r} m_y \;=\; t^r + \sum_{k=0}^{r-1} \frac{m_y[k]}{a^{r-k}} t^k \;\in\; E[t]$$

such that $m_u(u) = 0$. We claim that m_u truly is the minimal polynomial of u: If $h \in E[t]$ is any

other polynomial with $h(u) = 0$ and $d := \deg(h) \geq 0$, then in $F[t]$ we have

$$0 \;=\; \alpha(a)^d h(u) \;=\; \frac{y^d}{u^d} \sum_{k=0}^{d} h[k] u^k \;=\; \sum_{k=0}^{d} h[k] \alpha(a)^{d-k} y^k$$

The latter is a polynomial in $E[t]$ that turns y to 0. Hence m_y divides this polynomial $m_y \mid a^d h$ in $E[t]$. By construction we have $m_u = (1/a^r) m_y$ and hence $m_y = a^r m_u$. Thus we have

$$a^r m_u \;\mid\; a^d h \;\text{ in } E[t]$$

As $0 \neq a \in E$ we can just omit it. Then we have $m_u \mid h$ and as this is true for any polynomial $h \in E[t]$, $h \neq 0$ we have found $m_u E[t] = \{\, h \in E[t] \mid h(u) = 0 \,\}$, that is m_u is the minimal polynomial of u. But as $u \in S$, $S : R$ is integral and R is a normal domain we know $m_u \in R[t]$ by (8.37) again. That is all the coefficients of m_u are elements of R

$$\forall\, k \in 0 \ldots r-1 \;\;:\;\; m_u[k] \;=\; \frac{m_y[k]}{a^{r-k}} \;\in\; R$$

That is $a^{r-k} m_u[k] = m_y[k] \in \mathfrak{p}_0$. Suppose $m_u[k] \in \mathfrak{p}_0$ for all $k \in 0 \ldots r-1$, then we had

$$u^r \;\;=\;\; -\sum_{k=0}^{r-1} m_u[k]\, u^k \;\;\in\;\; \mathfrak{p}_0 S$$

But as $\mathfrak{p}_0 \subseteq \mathfrak{p}_0$ we have $\mathfrak{p}_0 S \subseteq \mathfrak{p}_1 S$. And $\mathfrak{p}_1 S = (\mathfrak{q}_1 \cap R) S \subseteq \mathfrak{q}_1$ is generally true, by (8.15). Together this is $\mathfrak{p}_0 S \subseteq \mathfrak{q}_1$ and thereby $u^r \in \mathfrak{q}_1$. But $\mathfrak{q}_1$ is a prime ideal thus we had $u \in \mathfrak{q}_1$ in contradiction to $u \in S \setminus \mathfrak{q}_1$. In conclusion there is some $k \in 0 \ldots r-1$ with $m_u[k] \notin \mathfrak{p}_0$. But we still have $a^{r-k} m_u[k] \in \mathfrak{p}_0$ and as $\mathfrak{p}_0$ is prime, this is $a \in \mathfrak{p}_0$. At long last, we have seen

$$\mathfrak{p}_0 S_{\mathfrak{q}_1} \cap R \;\;=\;\; \mathfrak{p}_0$$

- Recall that we regarded $S_{\mathfrak{q}_1} : R$ as a ring extension (under α_1) here. The identity $\mathfrak{p}_0 S_{\mathfrak{q}_1} \cap R = \mathfrak{p}_0$ is property (a) of the equivalencies in (8.15). Thus we have (b), too which is: There is a prime ideal $\overline{\mathfrak{q}}_0 \in \operatorname{Spec}(S_{\mathfrak{q}_1})$ such that $\overline{\mathfrak{q}}_0 \cap R = \mathfrak{p}_0$. As $\overline{\mathfrak{q}}_0$ is a prime ideal of $S_{\mathfrak{q}_1}$ it corresponds to a prime ideal $\mathfrak{q}_0 = \overline{\mathfrak{q}}_0 \cap S$ of S that satisfies $\mathfrak{q}_0 \cap \big(S \setminus \mathfrak{q}_q\big) = \emptyset$. Refer to (2.129) for details on this correspondence. Then by (8.18) we also get

$$\mathfrak{q}_0 \cap R \;=\; \big(\overline{\mathfrak{q}}_0 \cap S\big) \cap R \;=\; \overline{\mathfrak{q}}_0 \cap R \;=\; \mathfrak{p}_0$$

 As $\mathfrak{q}_0$ and $S \setminus \mathfrak{q}_q$ are disjoint, we have $\mathfrak{q}_0 \subseteq \mathfrak{q}_1$. Now suppose we even had $\mathfrak{q}_0 = \mathfrak{q}_1$, then we also had $\mathfrak{p}_0 = \mathfrak{q}_0 \cap R = \mathfrak{q}_1 \cap R = \mathfrak{p}_1$ in contradiction to $\mathfrak{p}_0 \subset \mathfrak{p}_1$. Thus we also have $\mathfrak{q}_0 \subset \mathfrak{p}_1$ and are done - under the assumption, that S was an integral domain.

- So let us now regard the case of an arbitrary commutative ring S (such that S is torsion-free, as an R-module). Let $\mathfrak{a} := 0 \trianglelefteq_{\mathrm{i}} S$, then $\mathfrak{a} \subseteq \mathfrak{q}_1$ Thus by (2.18.(iv)) there is a minimal prime ideal $\mathfrak{b}$ of S, that also satisfies $\mathfrak{b} \subseteq \mathfrak{q}_1$. And by (2.19) such an ideal is contained in the zero-divisors of S

$$\mathfrak{b} \;\subseteq\; \mathrm{zd}(S) \;=\; \{\, s \in S \mid \exists\, x \in S : x \neq 0, sx = 0 \,\}$$

Now consider any $a \in R$ with $\alpha(a) \in \mathrm{zd}(S)$. That is there is some $x \in S$ such that $x \neq 0$ but $ax = \alpha(a) \cdot x = 0$. By assumption S is R torsion free, that is $ax = 0$ implies $a = 0$ or $x = 0$. As $x \neq 0$ this means $a = 0$ and therefore $\alpha^{-1}(\mathrm{zd}(S)) = \{0\}$. In particular

$$\mathfrak{b} \cap R \;=\; 0$$

Recall that $\alpha : R \hookrightarrow S$ is injective and regard $\pi : S \twoheadrightarrow S/\mathfrak{b}$ defined by $\pi(x) := x + \mathfrak{b}$. Analogous to the above let $\alpha_1 := \pi\alpha$, that is $\alpha_1 : R \to S/\mathfrak{p} : a \mapsto \alpha(a) + \mathfrak{b}$. Suppose $\alpha_1(a) = 0$ that is $\alpha(a) \in \mathfrak{b}$, then $a \in \mathfrak{b} \cap R$ such that $a = 0$. That is $\mathrm{kn}(\alpha_1) = 0$ and hence α_1 is injective again.

- We regard $S_1 : R$ as a ring extension under α_1. This clearly is an integral extension, but you can also use (8.29.(iv)) and note that $\mathfrak{b} \cap R = 0$. As $\mathfrak{b} \subseteq \mathfrak{q}_1$ we get a corresponding prime ideal $\overline{\mathfrak{q}}_1 := \mathfrak{q}_1/\mathfrak{b} \in \mathrm{Spec}(S_1)$. By assumption we have $\mathfrak{q}_1 \cap R = \mathfrak{p}_1$ and hence

$$\overline{\mathfrak{q}}_1 \cap R \;=\; \{\, a \in R \mid \alpha(a) + \mathfrak{b} \in \overline{\mathfrak{q}}_1 \,\} \;=\; \{\, a \in R \mid \alpha(a) \in \mathfrak{q}_1 \,\} \;=\; \mathfrak{q}_1 \cap R \;=\; \mathfrak{p}_1$$

Now note that $S_1 := S/\mathfrak{b}$ is an integral domain, as $\mathfrak{b}$ was a prime ideal. Also S_1 is torsion-free, as it is an integral domain and α_1 is injective. Therefore we can use the case above and find a prime ideal $\overline{\mathfrak{q}}_0$ of S_1 such that $\overline{\mathfrak{q}}_0 \subset \overline{\mathfrak{q}}_1$ and $\overline{\mathfrak{q}}_0 \cap R = \mathfrak{p}_0$. By the correspondence theorem of ideals again, this is of the form $\overline{\mathfrak{q}}_0 = \mathfrak{q}_0/\mathfrak{b}$ for some $\mathfrak{b} \subseteq \mathfrak{q}_0 \in \mathrm{Spec}(S)$. Hence $\mathfrak{q}_0 \subset \mathfrak{q}_1$ follows immediately. And as before we conclude $\mathfrak{q}_0 \cap R = \mathfrak{p}_0$ by

$$\mathfrak{p}_0 \;=\; \overline{\mathfrak{q}}_0 \cap R \;=\; \{\, a \in R \mid \alpha(a) + \mathfrak{b} \in \overline{\mathfrak{q}}_0 \,\} \;=\; \{\, a \in R \mid \alpha(a) \in \mathfrak{q}_0 \,\} \;=\; \mathfrak{q}_0 \cap R$$

□

Proof of (8.73):

(i) If $(\mathfrak{q}_0, \ldots, \mathfrak{q}_n) \in \mathrm{CPI}(S)$ is any chain of prime ideals of S, then we define $\mathfrak{p}_k := \mathfrak{q}_k \cap R$ for any $k \in 0 \ldots n$. Thereby we get $\mathfrak{p}_0 \subseteq \ldots \subseteq \mathfrak{p}_n$. Suppose we had $\mathfrak{p}_{k-1} = \mathfrak{p}_k$ for some $k \in 1 \ldots n$. As also $\mathfrak{q}_{k-1} \subseteq \mathfrak{q}_k$ (8.32.(iii)) would impliy $\mathfrak{q}_{k-1} = \mathfrak{q}_k$, which is untrue. Hence $(\mathfrak{p}_0, \ldots, \mathfrak{p}_n) \in \mathrm{CPI}(R)$ also is a chain of prime ideals and as this is true for any CPI of S we conclude

$$\mathrm{kdim}(R) \;\geq\; \mathrm{kdim}(S)$$

Conversely we start with a CPI $(\mathfrak{p}_0, \ldots, \mathfrak{p}_n)$ of R. By the lying over theorem (8.32.(i)) there is a prime ideal $\mathfrak{q}_0 \in \mathrm{Spec}(S)$ such that $\mathfrak{q}_0 \cap R = \mathfrak{p}_0$. By the Going up Theorem (8.32.(iv)) we have $\mathfrak{p}_1 \in \mathbb{V}(\mathfrak{p}_0) = \mathbb{V}(\mathfrak{q}_0 \cap R) = \Sigma(\mathbb{V}(\mathfrak{q}_0))$. That is there is some $\mathfrak{q}_1 \in \mathbb{V}(\mathfrak{q}_0)$ such that $\mathfrak{p}_1 = \Sigma(\mathfrak{q}_1) = \mathfrak{q}_1 \cap R$. Thereby $\mathfrak{q}_1 \in \mathbb{V}(\mathfrak{q}_0)$ means $\mathfrak{q}_0 \subseteq \mathfrak{q}_1$. If we had $\mathfrak{q}_0 = \mathfrak{q}_1$ then of course $\mathfrak{p}_0 = \mathfrak{q}_0 \cap R = \mathfrak{q}_1 \cap R = \mathfrak{p}_1$ which is false. Hence we have $\mathfrak{q}_0 \subset \mathfrak{q}_1$ and continuing that way we can construct a CPI $(\mathfrak{q}_0, \ldots, \mathfrak{q}_n)$ of S with $\mathfrak{q}_k \cap R = \mathfrak{p}_k$ for any $k \in 0 \ldots n$. In particular we have found a CPI of the same length in S and thereby also conclude

$$\mathrm{kdim}(S) \;\geq\; \mathrm{kdim}(R)$$

(ii) Let $\mathfrak{a} := \mathfrak{u} \trianglelefteq_{\mathrm{i}} S$ be the ideal lying under $\mathfrak{u} \trianglelefteq_{\mathrm{i}} S$. As $S : R$ is an integral extension we know from

(8.29.(iv)) that $S/\mathfrak{u} : R/\mathfrak{a}$ is integral, too. Thus the claim is just another case of (i).

(iii) If $\text{height}(\mathfrak{u}) = \infty$, then there is nothing to prove. If $s := \text{height}(\mathfrak{u}) < \infty$ is finite, we pick up a CPI $(\mathfrak{q}_0, \ldots, \mathfrak{q}_s)$ of minimal length in S, that satisfies $\mathfrak{u} \subseteq \mathfrak{q}_s$. Then - as in the first part of (i) above - $(\mathfrak{q}_0 \cap R, \ldots, \mathfrak{q}_s \cap R)$ is a CPI in R, that satisfies $\mathfrak{u} \cap R \subseteq \mathfrak{q}_s \cap R$. There may be even shorter CPI in R with $\mathfrak{u} \cap R \subseteq \mathfrak{p}_r$ but at least we can conclude $\text{height}(\mathfrak{u} \cap R) \leq s = \text{height}(\mathfrak{u})$, as we have found a CPI of length s satisfying $\mathfrak{u} \cap R \subseteq \mathfrak{p}_s$.

(iv) By (iii) it remains to prove $\text{height}(\mathfrak{q}) \leq \text{height}(\mathfrak{q} \cap R)$. Note that $\mathfrak{p} := \mathfrak{q} \cap R$ is a prime ideal of R. If $\text{height}(\mathfrak{p}) = \infty$, there is nothing to prove hence let $r := \text{height}(\mathfrak{p}) < \infty$ be finite and pick up a CPI $(\mathfrak{p}_0, \ldots, \mathfrak{p}_r)$ in R, such that $\mathfrak{p}_r = \mathfrak{p}$ and r is minimal with this property. Recall that $\mathfrak{q} \cap R = \mathfrak{p}$, then by the Going-down theorem (8.72.(iii)) there is a CPI $(\mathfrak{q}_0, \ldots, \mathfrak{q}_r)$ in S lying over $(\mathfrak{p}_0, \ldots, \mathfrak{p}_r)$, in particular $\mathfrak{q}_r = \mathfrak{q}$. That is $\text{height}(\mathfrak{q}) \leq r = \text{height}(\mathfrak{p}) = \text{height}(\mathfrak{q} \cap R)$. Thus we have both inequalities and hence equality.

□

Proof of (8.41):

(i) For (b) $\implies$ (a) let $m \in R[t]$ be a monic polynomial such that $m(ax) = 0$ and let $d := \deg(m)$. Now define another, not necessarily monic, polynomial over R, by letting

$$f(t) \;:=\; \sum_{k=0}^{d} m[k]a^k t^k$$

As $f[d] = a^d m[d] = a^d$ and $a \neq 0$ and $\text{NIL}(R) = 0$ we have $f[d] \neq 0$ such that $f \neq 0$. Then it is clear, that $f(x) = m(ax) = 0$ and hence we have shown, that x is algebraic over R.

Conversely, for (a) $\implies$ (b), let $f \in R[t]$ be a polynomial with $f \neq 0$ and $f(x) = 0$. Also let $d := \deg(f)$ and $a := f[d]$. Then $a \neq 0$ and as $f(x) = 0$ we also have $d \geq 1$. Again we define another polynomial, this time

$$m(t) \;:=\; t^d + \sum_{k=0}^{d-1} f[k]a^{d-1-k}t^k$$

Then $m(ax) = a^d x^d + f[d-1]a^0(ax)^{d-1} + \cdots + f[0]a^{d-1} = a^{d-1}(ax^d + f[d-1]x^{d-1} + \cdots + f[0]) = a^{d-1}f(x) = 0$. That is m is a monic polynomial satisfying $m(ax) = 0$ and hence ax is integral over R.

(ii) First of all, we have 0_S and $1_S \in \text{alg}(S : R)$, as $f(t) = t$ and $g(t) = t - 1_R$ satisfy $f(0_S) = 0_S$ and $g(1_S) = 1_S - 1_S = 0_S$ respectively. So it remains to verify, that for any x, $y \in \text{alg}(S : R)$ and any $r \in R$ we have $x + y$, xy and $rx \in \text{alg}(S : R)$ again.

Yet by (i) $x \in \text{alg}(S : R)$ means $ax \in \text{int}(S : R)$ for some $a \in R$ with $a \neq 0$. Likewise $by \in \text{int}(S : R)$ for some $b \in R$ with $b \neq 0$. Yet by (8.30.(vi)) we know, that $\text{int}(S : R)$ is a sub-ring of S. Thus we find $ab(xy) = (ax)(by) \in \text{int}(S : R)$ again. Now $ab \neq 0$, as R was assumed to be an integral domain, and hence $xy \in \text{alg}(S : R)$ by (i) again. In particular $rx = (r1_S)x \in \text{alg}(S : R)$. Also

$ab(x+y) = b(ax) + a(by) \in \mathrm{int}(S:R)$ such that $x+y \in \mathrm{alg}(S:R)$. Altogether $\mathrm{alg}(S:R)$ is a sub-algebra of S.

(iii) Let us assume that $S : R$ is algebraic, then we first prove the isomorphism property: Clearly $U^{-1}S \to \mathrm{quot}(S)$ given by $x/u \mapsto x/u$ is a well-defined homomorphism. And as S (and hence R) is an integral domain $x/u = y/v$ is equivalent to $vx = uy$. As this is true in $U^{-1}S$ and $\mathrm{quot}(S)$ alike, this also is the injectvity. For the surjectivity we are given any $x/y \in \mathrm{quot}(S)$, that is x, $y \in S$ with $y \neq 0$. Let us abbreviate $E := \mathrm{quot}(R) = U^{-1}R$, which is a field, and regard the extension $U^{-1}S : E$. As $S : R$ is algebraic we have y is algebraic over R. In particular $y/1 \in U^{-1}S$ is algebraic over E. But E is a field, so (8.30.(vii)) tells us, that $E[y/1]$ is a field, too. In particular $y'/u := (y/1)^{-1} \in E[y/1] \subseteq U^{-1}S$. Then it is clear, that $(xy')/u \mapsto x/y$, as $(xy')y = xu$.

Now abbreviate $E := \mathrm{quot}(R)$ (as we did before) and $F := \mathrm{quot}(S)$ and let us prove that $F : E$ is algebraic, too (under the assumption that $S : R$ is algebraic, still). As we have just seen: If $x/y \in F$ then there is some $s \in S$ and $u \in R$ with $u \neq 0$, such that $x/y = s/u$. Then s is algebraic over R, say $f(s) = 0$ for some $f \in R[t]$ with $f \neq 0$. Let $d := \deg(f)$ and

$$g(t) \;:=\; \sum_{k=0}^{d} \frac{f[k]u^k}{1} t^k \;\in\; E[t]$$

then $g(s/u) = f(s)/1 = 0$ and $\deg(g) = \deg(f) \geq 0$, such that $x/y = s/u$ is algebraic over E, as well. Altogether $F : E$ is algebraic.

Conversely, if we start with $F : E$ algebraic and consider any $s \in S$, then there is some polynomial $g \in E[t]$ such that $g \neq 0$ but $g(s/1) = 0$. Let $d := \deg(g)$ and for any $k \in 0 \ldots d$ let $g[k] = a_k/u_k$. Then take $u := u_0 u_1 \ldots u_d \in R$ with $u \neq 0$ such that $f := ug \in R[t]$. Then $f(s) = ug(s/1) = 0$, such that s is algebraic over R, too. As this is true for any $s \in S$ we have established $S : R$ to be algebraic.

(iv) If $T : R$ is algebraic, then any $z \in T$ is algebraic over R. In particular any $y \in S \subseteq T$ is algebraic over R, such that $S : R$ is algebraic, too. Also, as $R \subseteq S$ we find $z \in T$ to be algebraic over S, as well. And that is $T : S$ is algebraic, again.

Conversely let us abbreviate $E := \mathrm{quot}(R)$, $F := \mathrm{quot}(S)$ and $G := \mathrm{quot}(T)$. If now $S : R$ and $T : S$ are algebraic, then so are $F : E$ and $G : F$, according to (iii). But as E and F are fields, this is the same, as $F : E$ and $G : F$ being integral. Now use (8.31.(ii)) to find $G : E$ integral. In particular $G : E$ is algebraic, such that $T : R$ is algebraic again, by another dose of (iii).

(v) As $T : R$ is finitely generated, there are some $y_1, \ldots, y_n \in T$ such that $T = R[y_1, \ldots, y_n]$. And as $T : S$ if finite, there are some $x_1, \ldots, x_m \in T$, such that $T = \mathrm{Lh}_S\{ x_1, \ldots, x_m \}$. Combining these properties, we find some $a_{r,k} \in S$ and $b_{i,j,k} \in S$, such that for any $r \in 1 \ldots n$ and any $i, j \in 1 \ldots m$, we get

$$\begin{aligned} y_r &= \sum_{k=1}^{m} a_{r,k} x_k \\ x_i x_j &= \sum_{k=1}^{m} b_{i,j,k} x_k \end{aligned}$$

The sets $A := \{ a_{r,k} \mid r \in 1 \ldots n, k \in 1 \ldots n \}$ and $B := \{ b_{i,j,k} \mid i,j,k \in 1 \ldots m \} \subseteq S$ are finite, that is $S_0 := R[A \cup B]$ is finitely generated. But R is a noetherian ring, so the Hilbert Basis theorem tells us, that S_0 is noetherian, as well. So if we pick up any $u \in T = R[y_1, \ldots, y_n]$ there is some polynomial $g \in R[t_1, \ldots, t_n]$ such that $u = g(y_1, \ldots, y_n)$. The y_r are $R[A]$-linear combinations of the x_k. Thus $u = g(y_1, \ldots, y_n)$ is an $R[A]$-linear combination over products of the form $x_{\alpha(1)} \ldots x_{\alpha(s)}$. And by induction on s it is clear, that any product $x_{\alpha(1)} \ldots x_{\alpha(s)}$ can be written as an $R[B]$-linear combination of $\{ x_1, \ldots, x_m \}$. Altogether we can write u as an S_0-linear combination of $\{ x_1, \ldots, x_m \}$. And as this is true for any $u \in T$, we get

$$T \;=\; \mathsf{Lh}_{S_0}\{ x_1, \ldots, x_m \}$$

As S_0 is a noetherian ring and T is a finitely generated S_0-module, we get, that T is a noetherian S_0-module. As S is an intermediate ring it in particular is a submodule $S \leq_{\mathsf{m}} T$ and hence S is a finitely generated S_0 module. In particular $S : S_0$ is a finitely generated S_0-algebra (using the same generators). But $S_0 : R$ is finitely generated by construction, so combining this we find, that $S : R$ is finitely generated.

□

Proof of (8.45):

- We abbreviate $P := R[U]$ the intermediate ring generated by $U \subseteq S$ and begin by proving (i): In (a) $\iff$ (b) the definition $U \vdash x$ means that there is some polynomial $f \in P[t]$ such that $f \neq 0$ but $f(x) = 0$. But this is precisely the definition of x being algebraic overP and hence $x \in \mathsf{alg}(S : P)$. And (b) $\iff$ (c) has already been proved in (8.41.(i)) under the assumption $\mathrm{NIL}(R) = 0$ only. It remains to verify (b) $\iff$ (d): If $P[x] = R[U \cup \{ x \}]$ is algebraic over $P = R[U]$, then in particular x is algebraic over U such that we have (b). Conversely, as $P \subseteq S$ and S is an integral domain, P is an integral domain, too. Therefore by (8.41.(ii)) $\mathsf{alg}(S : P)$ is a sub-ring of S. In particular $P[x] \subseteq \mathsf{alg}(S : P)$. And this again means $P[x] : P$ is an algebraic ring extension.

- In order to prove (ii) we have to establish the properties (D1) to (D4) of a dependence relation. We can do (D1) to (D3) right away, but (D4) will require (iii). So we have to interject the proof of this. We start with (D1), that is: $U \vdash u$ for any $u \in U$. This is easy: Let $P := R[u]$, then is particular $u \in P$ and hence $f(t) := t - u \in P[t]$. Then f is monic and $f(u) = 0$, such that u is algebraic (even integral) over P. This means $U \vdash u$.

- Let us continue, with (D2), that is: If $U \vdash x$ then there is some finite subset $U_x \subseteq U$ such that $U_x \vdash x$ already:

 Let $P := R[U]$, then by definition $U \vdash x$ means, that there is some $f \in P[t]$ such that $f \neq 0$ but $f(x) = 0$. Let $d := \deg(f)$, then $f[d] \neq 0$ and $f[k] \in P = R[U]$ for any $k \in \mathbb{N}$. By construction of $R[U]$ this means, that for any k there is a finite subset $U_k \subseteq U$ such that $f[k] \in R[U_k]$. Now let

 $$U_x \;:=\; \bigcup_{k=0}^{d} U_k$$

 Then U_x is finite, as well, and as $U_k \subseteq U_x$ we have $f[k] \in R[U_x]$ for any $k \in 0 \ldots d$. Therefore

$f = f[d]t^d + \cdots + f[1]t + f[0] \in R[U_x][t]$ and as $f[d] \neq 0$ and $f(x) = 0$, by assumption we have found $U_x \vdash x$.

- For (D3) we are given two subsets $V, U \subseteq S$, such that $V \vdash U$ and $U \vdash x$. That is we have $V \vdash u$ for any $u \in U$. Then we need to show $V \vdash x$:

 By assumption we have $V \vdash u$, which is $u \in \mathrm{alg}(S : R[V])$ by (i), for any $u \in U$. That is we have $U \subseteq \mathrm{alg}(S : R[V])$. Clearly this means $U \cup V \subseteq \mathrm{alg}(S : R[V])$, as $V \subseteq \mathrm{alg}(S : R[V])$ is a given. As S is an integral domain and $R[V]$ is a sub-ring of S, it is an integral domain, too. Hence by (8.41.(ii)) $\mathrm{alg}(S : R[U])$ is a ring again and therefore $R[U \cup V] \subseteq \mathrm{alg}(S : R[V])$. That is the extension $R[U \cup V] : R[V]$ is algebraic.

 But we also have $U \vdash x$ such that x is algebraic over $R[U]$. In particular x is algebraic over $R[U \cup V]$ but then the entire set $U \cup V \cup \{ x \}$ is algebraic over $R[U \cup V]$. By (8.41.(ii)) we conclude, that $R[U \cup V \cup \{ x \}] : R[U \cup V]$ is an algebraic extension, again.

 Together we have that both $R[U \cup V \cup \{ x \}] : R[U \cup V]$ and $R[U \cup V] : R[V]$ are algebraic. But by (8.31.(iv)) this means, that $R[U \cup V \cup \{ x \}] : R[V]$ is algebraic. In particular x is algebraic over $R[V]$ and this finally is $v \vdash x$.

- Let us now prove (iii), before turning our attention to property (D4). In (a) $\Longrightarrow$ (b) we do not require U to be algebraic independent: We have $U \vdash x$, but by property (D2) it suffices to regard a finite set $U = \{ u_1, \ldots, u_n \}$ for this. Then $U \vdash x$ yields a polynomial $f \in P[t]$ (where $P := R[U]$ again) such that $f \neq 0$ but $f(x) = 0$. We write f in the following form

$$f \;=\; \sum_{k=0}^{d} f_k \, t^k$$

 for some $f_k \in P$ and $f_d \neq 0$. That is $f_k = g_k(u_1, \ldots, u_n)$ for some polynomials $g_k \in R[t_1, \ldots, t_n]$. Now define the polynomial

$$g \;:=\; \sum_{k=0}^{d} g_k(t_1, \ldots, t_n) \, t_{n+1}^k \;\in\; R[t_1, \ldots, t_n, t_{n+1}]$$

 As $f_d \neq 0$ we have $g_d \neq 0$ and hence $g \neq 0$. Yet we also have $g(u_1, \ldots, u_n, x) = f(x) = 0$, which means that $\{ u_1, \ldots, u_n, x \}$ is algebraic dependent. In particular $U \cup \{ x \}$ is algebraic dependent.

 Conversely assume U to be algebraic independent, but $U \cup \{ x \}$ to be algebraic independent. That is there is some polynomial $g \in R[t_1, \ldots, t_{n+1}]$ such that $g \neq 0$ but $g(u_1, \ldots, u_n, x) = 0$. Write g in the form

$$g \;:=\; \sum_{k=0}^{d} g_k(t_1, \ldots, t_n) \, t_{n+1}^k$$

 with $g_d \neq 0$. As U is algebraic independent $\{ u_1, \ldots, u_n \}$ is algebraic independent and hence $g_d \neq 0$ implies $g_d(u_1, \ldots, u_n) \neq 0$. Therefore, if we define

$$f(t) \;:=\; \sum_{k=0}^{d} g_k(u_1, \ldots, u_n) \, t^k \;\in\; P[t]$$

 we have $f \neq 0$ as $f[d] = g_d(u_1, \ldots, u_n) \neq 0$. Never the less $f(x) = g(u_1, \ldots, u_n, x) = 0$, such

that x is algebraic over $R[u_1, \ldots, u_n]$. In particular x is algebraic over $R[U]$, which is $U \vdash x$.

- It is time we concluded (ii) by proving property (D4): That is we have $U \vdash x$ but for some $u \in U$ we also have $U \setminus \{ u \} \nvdash x$. Then we need to show $\big(U \setminus \{ u \}\big) \cup \{ x \} \vdash u$.

 First of all, it suffices to regard finite U for this: From $U \vdash x$ we find a finite set $U_0 \subseteq U$, such that $U_0 \vdash x$, by (D2). Suppose we had $u \notin U_0$, then $U_0 \setminus \{ u \} = U_0$ such that $U_0 \setminus \{ u \} = U_0 \vdash x$ in contradiction to $U \setminus \{ u \} \nvdash x$. Thus we have $u \in U_0$ and $U_0 \setminus \{ u \} \nvdash x$. If we are now able to prove $\big(U_0 \setminus \{ u \}\big) \cup \{ x \} \vdash u$, then the claim follows immediately, as $U_0 \subseteq U$.

 In a next step we claim, that $\{ u \}$ is algebraically independent: Suppose not, then there was some polynomial $f \in R[t]$ with $f \neq 0$ but $f(u) = 0$. But this means u is algebraic over R and hence $\emptyset \vdash x$. In particular $\{ u \} \setminus \{ u \} \vdash x$, in contradiction to $U \setminus \{ u \} \nvdash x$. That is the following set is non-empty, as it contains $\{ u \}$ as an element:

$$\mathcal{Q} \;:=\; \{\, Q \subseteq U \mid u \in Q,\, Q \text{ is algebraically independent} \,\}$$

 Now choose some $Q \in \mathcal{Q}$ with a maximal number of elements. This is possible, as $Q \subseteq U$ and we only need to regard a finite U. Then we claim: $Q \vdash U$. To do this consider an arbitrary $s \in U$. If $s \in Q$, then we are done already, as $Q \vdash s$ by (D1). If $s \in U \setminus Q$ then $Q \subset Q \cup \{ s \}$. Thus, as $Q \in \mathcal{Q}$ is maximal we find, that $Q \cup \{ s \}$ is algebraically dependent. But as Q is alebraically independent we conclude $Q \vdash s$ from (iii). Altogether $Q \vdash s$ for any $s \in U$ and hence $Q \vdash U$.

 But from $Q \vdash U$ and $U \vdash x$ we conclude $Q \vdash x$ by (D3). Suppose we had $Q \setminus \{ u \} \vdash x$ then, as $Q \subseteq U$, we also had $U \setminus \{ u \} \vdash x$, which is untrue. Thus we have found a set $Q \subseteq U$ with the following properties

 (1) $Q \vdash x$

 (2) $Q \setminus \{ u \} \nvdash x$

 (3) Q is finite

 (4) Q is algebraically independent

 Let $Q = \{ q_1, \ldots, q_n \}$ and by renumbering we may also assume $u = q_1$. Then (1) turns into $\{ q_1, \ldots, q_n \} \vdash x$ and (2) turns into $\{ q_2, \ldots, q_n \} \nvdash x$. Using (iii) again this can be turned into:

 (1') $\{ q_1, \ldots, q_n, x \}$ is algebraically dependent

 (2') $\{ q_2, \ldots, q_n, x \}$ is algebraically independent

 repsectively. By (2') $Q' := \{ q_2, \ldots, q_n, x \}$ satisfies the prerequisite of (iii), so we can conclude $Q' \vdash q_1$ from (1'). But this is precisely $\big(Q \setminus \{ u \}\big) \cup \{ x \} = Q' \vdash u$.

- Now for (iv): In (a) $\implies$ (b) we may assume $k = 1$, for ease of notation. Let $P := R[u_2, \ldots, u_n]$ and suppose $f \in P[t]$ is a polynomial with $f(u_1) = 0$. Let $d \geq \deg(f)$, then for any $k \in 0 \ldots d$ we have $f[k] \in P$, that is $f[k] = g_k(u_2, \ldots, u_n)$ for some $g_k \in R[t_2, \ldots, t_n]$. Let

$$g(t_1, \ldots, t_n) \;:=\; \sum_{k=0} g_k(t_2, \ldots, t_n)\, t_1^k$$

Then $0 = f(u_1) = g(u_1, u_2, \ldots, u_n)$ and by assumption (a) this means $g = 0$. This is $g_k = 0$ and hence $f[k] = 0$ for any $k \in 0 \ldots d$. In turn $f = 0$ and hence $\{ u_2, \ldots, u_n \} \vdash u_1$ is untrue.

We prove (b) $\implies$ (c) by negation $\neg$ (c) $\implies$ $\neg$ (b): This is obvious: As for any $k \in 1 \ldots n$ we have $\{ u_1, \ldots, u_{k-1} \} \subseteq U \setminus \{ u_k \}$ the dependency $\{ u_1, \ldots, u_{k-1} \} \vdash u_k$ *non* (c) would also imply $U \setminus \{ u_k \} \vdash u_k$, which is *non* (b).

We close the circle, by (c) $\implies$ (a): Suppose there was some polynomial $f \in R[t_1, \ldots, t_n]$ such that $f \neq 0$, but $f(u_1, \ldots, u_n) = 0$ then we can choose k minimal, such that $f(u_1, \ldots, u_k) = 0$ for some $f \in R[t_1, \ldots, t_k]$ with $f \neq 0$. If we had $k = 1$ then u_1 would be algebraic over R, which is ruled out, as by (c) for $k = 1$ we have $\emptyset \nvdash u_1$. Therefore $k \geq 2$, such that we may write this polynomial, as

$$f(t_1, \ldots, t_k) \;=\; \sum_{i=0}^{d} f_i(t_1, \ldots, t_{k-1})\, t_k^i$$

with $f_d \neq 0$ and let $a_i := f_i(u_1, \ldots, u_{k-1}) \in P = R[u_1, \ldots, u_{k-1}]$. Now take $g(t) := a_d t^d + \cdots + a_1 t + a_0 \in P[t]$ then $g(u_k) = f(u_1, \ldots, u_k) = 0$. As k was minimal we have $a_d \neq 0$ and hence $g \neq 0$. But this would mean $\{ u_1, \ldots, u_{k-1} \} \vdash u_k$ in contradiction to (c).

□

Proof of (8.46):

(i) If (a) U is $\vdash$independent, then by definition we have $U \setminus \{ u \} \nvdash u$ for any $u \in U$. Suppose U was *not* algebraically independent, that is there is a finite subset $U_0 \subseteq U$, which is not algebraically independent. Hence we may choose a subset $\{ u_1, \ldots, u_n \} \subseteq U$ that is algebraically independent, but with a minimal number n of elements. So consider any polynomial $f \in R[t_1, \ldots, t_n]$ such that $f(u_1, \ldots, u_n) = 0$ for some $u_1, \ldots, u_n \in U$. Unless $f = 0$ there is some t_k occurring in f, for ease of notation, say $d := \deg_1(f) \geq 1$. Always the same idea: We write f in the form

$$f \;=\; \sum_{k=0}^{d} f_k(t_2, \ldots, t_n)\, t_1^k$$

for some $f_k \in R[t_2, \ldots, t_n]$ where $f_d \neq 0$. As $\{ u_2, \ldots, u_n \}$ contains fewer than n elements, this set is algebraically independent and hence $f_d(u_2, \ldots, u_n) \neq 0$. Note that $n = 1$ is not a problem, in this case $f_d \neq 0 \in R$ already. Therefore $g(t) := f(t, u_2, \ldots, u_n) \in P[t]$ is a non-zero polynomial over $P = R[u_2, \ldots, u_n] \subseteq R[U \setminus \{ u_1 \}]$ such that $g(u_1) = 0$. This contradicts $U \setminus \{ u_1 \} \nvdash u_1$ and hence we conclude, that U *is* algebraically independent.

Let us commence, with (b) $\implies$ (c): That is we regard the evaluation homomorphism ε from $R[t_u \mid u \in U]$ to $R[U]$, that is defined by expansion of $\varepsilon(t_u) := u$

$$\varepsilon \,:\, R[t_u \mid u \in U] \to R[U] \,:\, t_u \mapsto u$$

By definition of $R[U]$ as the sub-ring generated by U this homomorphism is surjective. And $\varepsilon(f) = 0$ means $f(u_1, \ldots, u_n) = 0$ for some $u_i \in U$ - those u_i such that t_{u_i} occurs in f. But as U is algebraically independent, so is $\{ u_1, \ldots, u_n \}$ and therefore $f = 0$. This is $\mathrm{kn}(\varepsilon) = 0$, such that ε is

injective. Hence ε is an isomorphism.

We come full circle (c) $\implies$ (a): Pick any $u \in U$, then we need to show $U \setminus \{ u \} \nvdash u$. If we had $U \setminus \{ u \} \vdash u$, then we already had $\{ u_2, \ldots, u_n \} \vdash u$ for some finite subset $\{ u_2, \ldots, u_n \} \subseteq U$. That is there, is a polynomial $g(t) \in R[u_2, \ldots, u_n][t]$ such that $g \neq 0$ but $g(u) = 0$. Say g is

$$g(t) \;=\; \sum_{k=0}^{d} g_k(u_2, \ldots, u_n)\, t^k$$

where $g_d(u_2, \ldots, u_n) \neq 0$. As ε is an isomorphism of R-algebras we can apply $\varepsilon^{-1} : u_i \mapsto t_i := t_{u_i}$. If we also let $t_1 := \varepsilon^{-1}(u)$, that is $t_1 := t_u$ then $g(u) = 0$ turns into

$$0 \;=\; \varepsilon^{-1}\big(g(u)\big) \;=\; \sum_{k=0}^{d} g_k(t_2, \ldots, t_n)\, t_1^k$$

But this is a polynomial in $R[t_2, \ldots, t_n][t_1]$. And the polynomial only is 0, iff all its coefficients $g_k(t_2, \ldots, t_k)$ are. In particular $g_d = 0$, but this contradicts $g_d(u_2, \ldots, u_n) \neq 0$. Thus $U \setminus \{ u \} \vdash u$ cannot occur and hence U is $\vdash$independent.

(ii) If $\langle U \rangle = \{ x \in S \mid U \vdash x \}$ is the set of elements of S, that are generated by U, under the relation of algebraic dependence, then by (8.45.(i)) we have $\langle U \rangle = \operatorname{alg}(S : R[U])$. But in fact $U \vdash x$ is precisely the definition of $x \in S$ being algebraic over $R[U]$. Hence $\langle U \rangle = S$ is the same, as $\operatorname{alg}(S : R[U]) = S$, which is the same as $S : R[U]$ being an algebraic extension.

(iii) (a) contains: U is $\vdash$independent and $U \vdash$generates S. Due to (i) and (ii) respectively, this translates into U is algebraically independent and $S : R[U]$ is algebraic. And this is precisely the sitation we called (b): U is a transcendence basis of $S : R$.

(iv) As in (ii) we have $\langle U \rangle = \operatorname{alg}(S : R[U])$ and want to show $\langle U \rangle = \langle U' \rangle$ that is $\operatorname{alg}(S : R[U]) = \operatorname{alg}(S : R[U'])$. By assumption we have $R[U'] \subseteq R[U]$ and thereby $\operatorname{alg}(S : R[U]) \supseteq \operatorname{alg}(S : R[U'])$. For the converse inclusion we regard any $x \in \overline{U} := \operatorname{alg}(S : R[U])$ and need to show $x \in \operatorname{alg}(S : R[U'])$. By definition $\overline{U} : R[U]$ is algebraic. But by assumption we also have, that $R[U] : R[U']$ is algebraic. Hence by (8.41.(iv)) $\overline{U} : R[U']$ is algebraic, too. That is $x \in \overline{U} \subseteq \operatorname{alg}(S : R[U'])$.

Together we have $\langle U \rangle = \langle U' \rangle$ and U' is independent, by assumption. Thus we can invoke the basis exchange theorem of dependence relations (3.57.(x)) to conclude that $V' := (V \setminus U) \cup U'$ is a basis. This means V' is a transcendence basis of $S : R$.

□

Proof of (8.48):

(vi) Items (i) to (v) are clear or have already been argued for in the example above. So we only prove (vi) and (vii) here: Let us first check, that U truly is algebraically independent, that is we consider some polynomial $f \in R[t_2, \ldots, t_n]$ such that $f(u_2, \ldots, u_n) = 0$. As $u_k = t_k + pA$ this is $f(u_2, \ldots, u_n) = f(t_2, \ldots, t_n) + pA = 0$. In turn we find some $q \in A$ such that $f = pq$.

Let $d := \deg_1(p)$ which is $d \geq 1$, by assumption. If we had $f \neq 0$ then also $q \neq 0$, as A is an integral domain and thereby $0 = \deg_1(f) = \deg_1(p) + \deg_1(q) \geq d \geq 1$. This is absurd, so we must have $f = 0$ and hence U is algebraically independent.

It remains to prove, that $S : R[U]$ is algebraic. Note that $S = R[U][u_1]$ and that the algebraic closure is an R-algebra, by (8.41.(ii)), as S is an integral domain (p is prime). Hence it suffices to prove, that u_1 is algebraic over $R[U]$. But as U is algebraically independent this is the same as $U \cup \{ u_1 \} = \{ u_1, u_2, \ldots, u_n \}$ being algebraically dependent - refer to (8.45.(iii)) for this. And this now is trivial: $p(u_1, \ldots, u_n) = p(t_1, \ldots, t_n) + pA = p + pA = 0 + pA$.

(vii) First of all any $u \in U$ is integral over $R[U']$, as it trivially satisfies a polynomial of the form $t^{m(u)} - u^{m(u)} \in R[U'][t]$. Then by (8.30.(iv)) $R[U] : R[U']$ is integral and hence algebraic. But by assumption $S : R[U]$ is algebraic, too, such that $S : R[U']$ is algebraic, by (8.41.(iv)) again. But U' is algebraically independent, too: Suppose we had $f(u_1^{m_1}, \ldots, u_n^{n_m}) = 0$ for some polynomial $f \in R[t_1, \ldots, t_n]$. Then define $g := f(t_1^{m_1}, \ldots, t_n^{n_m})$ to get $g(u_1, \ldots, u_n) = 0$. This implies $g = 0$, as U is algebraically independent and hence $f = 0$.

□

Proof of (8.49):

(i) Let $\Delta := \det(A)$, then we start with $\Delta \neq 0$ and need to prove, that $\{ w_1, \ldots, w_n \}$ is a transcendence basis of $S : R$ again: Let $A^\#$ be the adjugate matrix of A, then by (4.63.(iii)) we have $A^\# A = A A^\# = \Delta \mathbb{1}_n$. Let us now regard the endomorphisms $\varphi := \varphi_A$ and $\varphi^\# := \varphi_{A^\#}$, that is

$$\varphi : R[t_1, \ldots, t_n] \to R[t_1, \ldots, t_n] : t_i \mapsto [At]_i$$

$$\varphi^\# : R[t_1, \ldots, t_n] \to R[t_1, \ldots, t_n] : t_i \mapsto [A^\# t]_i$$

then we obtain $\varphi^\# \varphi(t_i) = \varphi \varphi^\#(t_i) = \Delta t_i$ - according to (7.56). Let us prove that the map defined by $t_i \mapsto \Delta t_i$ is injective: That is we consider any polynomial $f \in R[t_1, \ldots, t_n]$ such that

$$0 \;=\; f(\Delta t_1, \ldots, \Delta t_n) \;=\; \sum_{\alpha \in \mathbb{N}^n} f[\alpha] \Delta^{|\alpha|}\, t^\alpha$$

As this is 0 we have $f[\alpha]\Delta^{|\alpha|} = 0$ for any $\alpha \in \mathbb{N}^n$. But as R is an integral domain and $\Delta \neq 0$ by assumption, this means $f[\alpha] = 0$. And as this is true for any α this is $f = 0$, again. Thus $\varphi_\Delta(t_i) := \Delta t_i$ is injective and as $\varphi^\# \varphi = \varphi_\Delta$ this implies, that φ is injective. Likewise $\varphi \varphi^\# = \varphi_\Delta$ makes $\varphi^\#$ injective, too, but we do not require this.

Als $\{ v_1, \ldots, v_n \}$ is algebraically independent the homomorphism $\varepsilon_v : R[t_1, \ldots, t_n] \to R[v_1, \ldots, v_n]$ of evaluation, that is defined by expansion of $\varepsilon_v : t_i \mapsto u_i$ is an isomorphism, due to (8.46.(i)). Now consider $\{ w_1, \ldots, w_n \}$ and any polynomial $f \in R[t_1, \ldots, t_n]$ such that $f(w_1, \ldots, w_n) = 0$. That is

$$\begin{aligned} 0 \;&=\; \sum_{\alpha \in \mathbb{N}^n} f[\alpha]\, w^\alpha \;=\; \sum_{\alpha \in \mathbb{N}^n} f[\alpha] \prod_{i=1}^n [Av]_i^{\alpha_i} \\ &=\; \varepsilon_v \left(\sum_{\alpha \in \mathbb{N}^n} f[\alpha] \prod_{i=1}^n [At]_i^{\alpha_i} \right) \;=\; \varepsilon_v \left(\varphi \left(\sum_{\alpha \in \mathbb{N}^n} f[\alpha]\, t^\alpha \right) \right) \end{aligned}$$

Note that we denote $t = (t_1, \ldots, t_n)$, $v = (v_1, \ldots, v_n)$ and $w = (w_1, \ldots, w_n)$ all the time. Then $f(w_1, \ldots, w_n) = 0$ turns into $\varepsilon_v(\varphi(f)) = 0$ and therefore $f = 0$, as ε_v is bijective and φ is injective. That is $\{ w_1, \ldots, w_n \}$ is algebraically independent, too. Also for any $i \in 1 \ldots n$ let

$$g_i(t) \;:=\; \Delta t - [A^{\#} w]_i \;\in\; R[w_1, \ldots, w_n][t]$$

As $A^{\#} w = A^{\#}(Av) = (A^{\#} A)v = \Delta v$ we have $\Delta v_i = [A^{\#} w]_i$ and thereby $g_i(v_i) = 0$. That is v_i is algebraic over $R[w_1, \ldots, w_n]$. Yet S is an integral domain and $R[w_1, \ldots, w_n] \subseteq S$ such that (8.41.(ii)) tells us that $R[v_1, \ldots, v_n]$ is algebraic over $R[w_1, \ldots, w_n]$. But by assumption S is algebraic over $R[v_1, \ldots, v_n]$, too. Hence S is algebraic over $R[u_1, \ldots, u_n]$ by (8.41.(iv)) and this means $\{ w_1, \ldots, w_n \}$ is a transcendence basis of $S : R$.

While this was a little demanding the converse direction is free for the taking: Suppose $\Delta = 0$, then we have to show, that $\{ w_1, \ldots, w_n \}$ is not a transcendence basis of $S : R$. We will prove that $\{ w_1, \ldots, w_n \}$ is algebraically dependent. In fact it already is linearly dependent! As $\det(A) = 0$ the row vectors $r_i := \mathrm{row}_i(A) \in R^n$ of A are linearly dependent, as we have seen in (4.65.(ii)). That is there is a non-trivial tuple $(a_1, \ldots, a_n) \neq 0 \in R^n$ such that $a_1 r_1 + \cdots + a_n r_n = 0$. Note that $w_i = [Av]_i = \langle r_i \mid v \rangle$ such that we can insert this equation into the scalar product with v:

$$0 \;=\; \langle 0 \mid v \rangle \;=\; \langle a_1 r_1 + \cdots + a_n r_n \mid v \rangle \;=\; a_1 w_1 + \cdots + a_n w_n$$

In particular, if we take the polynomial $f = a_1 t_1 + \cdots + a_n t_n \in R[t_1, \ldots, t_n]$, then $f \neq 0$, as one of the a_i is non-zero, but $f(w_1, \ldots, w_n) = 0$. That is $\{ w_1, \ldots, w_n \}$ is algebraically dependant.

(ii) Let us abbreviate $E := \mathrm{QUOT}(R)$ and $F := \mathrm{QUOT}(R)$. Then we first prove, that $V/1$ is algebraically independent over E: That is we consider a polynomial $g \in E[t_1, \ldots, t_n]$ such that for some $v_1, \ldots, v_n \in V$ we have $g(v_1/1, \ldots, v_n/1) = 0$. As g is a polynomial over E all its coefficients are of the form $g[\alpha] = a_\alpha / b_\alpha$ for some a_α, $b_\alpha \in R$ with $b_\alpha \neq 0$. Also, as g is a polynomial, the set $A := \{ \alpha \in \mathbb{N}^n \mid a_\alpha \neq 0 \}$ is finite. Now define

$$b \;:=\; \prod_{\alpha \in A} b_\alpha \;\in\; R$$

Then $b \neq 0$, as all the $b_\alpha \neq 0$ and R is an integral domain (since $R \subseteq S$). Also let $\widehat{b}_\alpha := b / b_\alpha \in R$, then $bg[\alpha] = b\, a_\alpha / b_\alpha = a_\alpha \widehat{b}_\alpha \in R$ and take a look at the polynomial

$$f \;:=\; \sum_{\alpha \in A} a_\alpha \widehat{b}_\alpha \, t^\alpha \;\in\; R[t_1, \ldots, t_n]$$

Then it is clear, that $0 = bg(v_1/1, \ldots, v_n/1) = \sum_\alpha bg[\alpha] v^\alpha / 1 = \sum_\alpha a_\alpha \widehat{b}_\alpha v^\alpha / 1 = f(v_1, \ldots, v_n)/1$. That is $f(v_1, \ldots, v_n) = 0$ and as V is algebraically independent, this implies $f = 0$. This means $a_\alpha \widehat{b}_\alpha = 0$ for any $\alpha \in A$. But as both a_α and $\widehat{b}_\alpha \neq 0$ are non-zero, this can only mean $A = \emptyset$. And this is $g = 0$. Hence $V/1$ is algebraically independent, as well.

It remains to prove, that $F : E[V]$ is algebraic: That is we consider any $x/y \in F$, hence x, $y \in S$

with $y \neq 0$. As $S : R[U]$ is algebraic, there is some polynomial $f(t) \in R[V][t]$ such that $f \neq 0$, but $f(x) = 0$. Say $d := \deg(f)$, then we define the polynomial

$$g(t) \;:=\; \sum_{k=0}^{d} \frac{f[k]y^k}{1} t^k \;\in\; E[V/1][t]$$

Then it is clear, that $g(x/y) = \sum_k (f[k]y^k/1)(x^k/y^k) = \sum_k f[k]x^k/1 = f(x)/1 = 0$. And as $f[d] \neq 0$ and $y \neq 0$ we also have $g[d] = f[d]y^d \neq 0$ such that $g \neq 0$. That is x/y is algebraic over $E[V/1]$ (even over $R[V/1]$). As this is true for any $x/y \in F$ the whole extension $F : E[V/1]$ is algebraic and altogether $V/1$ is a transcendence basis of $F : E$.

(iii) By assumption $S : R[V]$ and $R : Q[U]$ are algebraic, that is any $r \in R$ is algebraic over $Q[U]$. In particular any $r \in R$ is algebraic over the larger ring $Q[U \cup V]$. Also any $v \in V$ is algebraic (even integral) over $Q[U \cup V]$. That is we have found

$$R \cup V \quad \subseteq \quad \mathrm{alg}\big(S : Q[U \cup V]\big)$$

Yet the algebraic closure $\mathrm{alg}(S : Q[U \cup V])$ is a Q-sub-algebra of S, by (8.41.(ii)), such that $R[V] \subseteq \mathrm{alg}(S : Q[U \cup V])$. That is $R[V] : Q[U \cup V]$ is algebraic. Now as $S : R[V]$ is algebraic, too, we conclude that $S : Q[U \cup V]$ is algebraic, according to (8.41.(iv))

It remains to prove that $U \cap V = \emptyset$ and that $U \cup V$ is algebraically independent. Both will be apparent from the following reasoning: Suppose we had some polynomial $f \in Q[s_1, \ldots, s_m, t_1, \ldots, t_n]$ such that for some $u_i \in U$ and some $v_j \in V$ would yield $f(u_1, \ldots, u_m, v_1, \ldots, v_n) = 0$. Then we would write this term in the form

$$f(u_1, \ldots, u_m, v_1, \ldots, v_n) \;=\; \sum_{\beta \in \mathbb{N}^n} f_\beta(u_1, \ldots, u_m)\, v^\mu$$

That is we have a polynomial term over $Q[U]$ that turns $v_1, \ldots, v_n$ to zero. But by assumption V is algebraically independent over R and $Q[U] \subseteq R$. Thus we conclude $f_\beta(u_1, \ldots, u_m) = 0$. Hereby $f_\beta \in Q[s_1, \ldots, s_m$ is a polynomial again. So as U is algebraically independent over Q, we conclude $f_\beta = 0$. Thus the entire $f = 0$ is zero.

Suppose there was some $x \in U \cap V$, then we could have taken $f(s,t) := s - t \in Q[s,t]$. Then $f \neq 0$ but $f(x,x) = 0$ which we have just proven to be impossible. So as $U \cup V$ is a transcendence basis and $U \cap V = \emptyset$ we conclude the formula for the transcendence degrees in the claim above.

□

Proof of (8.50):

(i) As ε is a surjective homomorphism of R-algebras, by construction, (b) in truth is equivalent, to ε being injective. And for a homomorphism this equivalent to $\mathrm{kn}(\varepsilon) \subseteq 0$. Explicitly this is the implication $f(u_1, \ldots, u_n) = 0 \implies f = 0$, for any polynomial $f \in R[t_1, \ldots, t_n]$. And this is property (a) - U being algebraically independent - already.

(ii) To say that $v_0 \in V$ is algebraic over $R[U \cup V \setminus \{ v_0 \}]$ means that v_0 satisfies a non-zero polynomial whose coefficients are in this intermediate ring

$$\sum_{k=0}^{d} g_k v_0^k \;=\; 0 \;\text{ where }\; g_k \in R[U \cup V \setminus \{ v_0 \}]$$

That is g_k is a polynomial expression over $U \cup V \setminus \{ v \}$ and as such only depends on finitely many variables $u_i \in U$ and $v_j \in V \setminus \{ v_0 \}$. And as we only have finitely many g_k the collection of this is finite again. Say $u = (u_1, \ldots, u_m) \in U^m$ and $v = (v_1, \ldots, v_n) \in V^n$ are these variables, that is $g_k = f_k(u_1, \ldots, u_m, v_1, \ldots, v_n)$ for some $f_k \in R[s_1, \ldots, s_m, t_1, \ldots, t_n]$. Inserting this the above expression turns into

$$\sum_{k=0}^{d} \sum_{\alpha \in \mathbb{N}^m} \sum_{\beta \in \mathbb{N}^n} f_k[\alpha, \beta]\, u^\alpha v^\beta v_0^k \;=\; 0$$

This is a polynomial expression in $\{ u_1, \ldots, u_m, v_0, v_1, \ldots, v_n \} \subseteq U \cup V$ over R. And as $g_d \neq 0$ we have $f_d \neq 0$ and hence there are some α and β with $f_d[\alpha, \beta] \neq 0$. That is $U \cup V$ is algebraically dependent over R.

(ii) If $U \cup V$ is algebraically dependent, then there are $u = (u_1, \ldots, u_m) \in U^m$ and $v = (v_1, \ldots, v_n) \in V^n$ such that there is a non-zero polynomial $f \in R[s_1, \ldots, s_m, t_1, \ldots, t_n]$ such that $f(u, v) = 0$. That is we have an expression of the form

$$f(u,v) \;=\; \sum_{\alpha \in \mathbb{N}^m} \sum_{\beta \in \mathbb{N}^n} f[\alpha, \beta]\, u^\alpha v^\beta \;=\; 0$$

Let us take $n \in \mathbb{N}$ to be the minimal minimal number such that there is such a combination $(u, v) \in U^m \times V^n$. Suppose we had $f[\alpha, \beta] = 0$ for all $\beta \neq 0$. Then this would be a polynomial relation $\sum_\alpha f[\alpha, 0] u^\alpha = 0$ containing u only. As U is algebraically independent this means $f[\alpha, 0] = 0$ for any $\alpha \in \mathbb{N}^m$, too. But then we had $f = 0$, which we did not. Thus there have to be some $\alpha_0 \in \mathbb{N}^m$ and some $\beta_0 \in \mathbb{N}^n$ such that $\beta_0 \neq 0$ and $f[\alpha_0, \beta_0] \neq 0$. Hence there is some $j \in 1 \ldots n$ such that the j-th component of β_0 is 1 at least. For ease of notation let us assume $j = 1$, that is β_0 is of the form $\beta_0 = (r, \beta_0')$ with $r \geq 1$. Then we expand f as a polynomial in $R[s_1, \ldots, s_m, t_2, \ldots, t_n][t_1]$ to find an expression of the form

$$0 \;=\; f(u,v) \;=\; \sum_{k=0}^{d} \left(\sum_{\alpha \in \mathbb{N}^m} \sum_{\beta' \in \mathbb{N}^{n-1}} f[\alpha, \beta]\, u^\alpha v^{\beta'} \right) v_1^k$$

Now for $\alpha = \alpha_0$ and $(r, \beta') = \beta_0$ we have $f[\alpha, \beta] \neq 0$. As n was minimal the corresponding expression in brackets is non-zero. But this is a polynomial expression in v_1 over $R[u_1, \ldots, u_m, v_2, \ldots, v_n]$. In particular v_1 is algebraic over $R[U \cup V \setminus \{ v_1 \}]$.

(iii) Let $\mathcal{Z} := \{ V \subseteq S \mid U \subseteq V,\, V \text{ is algebraically independent over } R \}$. As $U \in \mathcal{Z}$ we have $\mathcal{Z} \neq \emptyset$. Now suppose $(V_i) \subseteq \mathcal{Z}$ is a chain of algebraically independent sets in S, where $i \in I$, then take

$$V \;:=\; \bigcup_{i \in I} V_i$$

We claim, that V is algebraically independent, again: To do this it suffices to regard finitely many elements $\{ v_1, \ldots, v_n \} \subseteq V$. By construction $v_k \in V_{i(k)}$ for some $i(k) \in I$. As the V_i form a chain we may assume (by renumbering the v_i) that $V_{i(1)} \subseteq \ldots \subseteq V_{i(n)}$. Then we have $\{ v_1, \ldots, v_n \} \subseteq V_{i(n)}$. But as $V_{i(n)}$ is algebraically independent, so is $\{ v_1, \ldots, v_n \}$ and this is what we aimed for:

Hence we may invoke the lemma of Zorn to find a maximal element $U^* \in \mathcal{Z}$. By construction this U^* satisfies (1) and (2) and it only remains to prove (3): Consider any $s \in S$, if $s \in U^*$ then clearly s is algebraic over $R[U^*]$, as it satisfies the polynomial $t - s \in R[U^*][t]$. Otherwise, if $s \notin U^*$, then $U^* \subset U^* \cup \{ s \}$ is a truly larger set. By maximality of U^* this means that $U^* \cup \{ s \}$ is algebraically dependent over R. But by (ii) this means that s is algebraically dependent over $R[U^*]$. Thus in any case $s \in S$ is algebraic over $R[U^*]$ and this is property (3).

(iv) Let $V_0 := V \setminus U$ such that $V' = V_0 \cup U'$. We need to show that $S : R[V']$ is integral again. Any $v \in V_0$ is integral over $R[V_0]$, as it satisfies the polynomial $t - v_0$. As $R[V_0] \subseteq R[V']$ it also is integral over $R[V']$. Also any $u \in U$ is integral over $R[U']$, by assumption (2). And as $R[U'] \subseteq R[V']$, we see that u is integral over $R[V']$. That is we have

$$V \;=\; V_0 \cup U \;\subseteq\; \mathrm{int}(S : R[V'])$$

And as the integral closure is a sub-ring of S, by (8.30.(iv)), we find $R[V] \subseteq \mathrm{int}(S : R[V'])$. That means $R[V] : R[V']$ is an integral extension. But $S : R[V]$ is integral, too, such that with (8.31.(ii)) we conclude, that $S : R[V']$ is an integral extension, again.

(v) In this case we need to prove, that V' is algebraically independent. Suppose V' was not, then there are finitely many elements $u' = (u'_1, \ldots, u'_m) \in U'^m$ and $v = (v_1, \ldots, v_n) \in V_0^n$ such that for some non-zero polynomial $f \in R[s_1, \ldots, s_m, t_1, \ldots, t_n]$ we have

$$f(u, v) \;=\; \sum_{\alpha \in \mathbb{N}^m} \sum_{\beta \in \mathbb{N}^n} f[\alpha, \beta]\, u'^{\alpha} v^{\beta} \;=\; 0$$

Take $g_\beta := \sum_\alpha f[\alpha, \beta]\, u'^{\alpha} \in R[U']$. As U' is algebraically independent and there are some α, β with $f[\alpha, \beta] \neq 0$ we also get $g_\beta \neq 0$ for this β. Now we rewrite the above equation in the form

$$\sum_{\beta \in \mathbb{N}^m} g_\beta\, v^{\beta} \;=\; 0$$

That is V_0 is algebraically dependent over $R[U']$. But by property (2) we have $R[U'] \subseteq R[U]$, such that V_0 is algebraically dependent over $R[U]$. That is there are some $u = (u_1, \ldots, u_m) \in U^m$ and $w = (w_1, \ldots, w_n) \in V_0^n$ such that

$$\sum_{\beta \in \mathbb{N}^n} \left(\sum_{\alpha \in \mathbb{N}^m} f[\alpha, \beta]\, u^{\alpha} \right) w^{\beta} \;=\; 0$$

As the $\sum_\alpha f[\alpha, \beta]\, u^{\alpha} \neq 0$ are non-zero, there are some α, β with $f[\alpha, \beta] \neq 0$. And therefore we have a polynomial relation between elements in V. But this contradicts V being algebraically independent and hence V' has to be algebraically independent, too.

□

Proof of (8.43):

- Let us first prove $xy^kA \subseteq xy^kE + x^2y^kB$: By construction any element of $a \in A$ is of the form $a = f(x, xy, \ldots, xy^n)$ for some $n \in \mathbb{N}$ and some polynomial $f \in E[t_0, t_1, \ldots, t_n]$. Therefore

$$xy^k a \;=\; xy^k f(x, xy, \ldots, xy^n) \;=\; xy^k \sum_{\alpha \in \mathbb{N}^{n+1}} f[\alpha](x, xy, \ldots, xy^n)^\alpha$$

 For any multi-index $\alpha \in \mathbb{N}^{n+1}$ let us denote $\omega(\alpha) := 0 \cdot \alpha_0 + 1 \cdot \alpha_1 + \cdots + n \cdot \alpha_n$. Then we clearly have $(x, xy, \ldots, xy^n)^\alpha = x^{|\alpha|}y^{\omega(\alpha)}$ such that we are able to find $xy^ka \in xy^kE + x^2y^kB$ from

$$\begin{aligned} xy^k a \;&=\; xy^k \sum_{\alpha \in \mathbb{N}^{n+1}} f[\alpha]\, x^{|\alpha|}y^{\omega(\alpha)} \;=\; xy^k \left(f[0] + \sum_{\alpha \neq 0} f[\alpha]\, x^{|\alpha|}y^{\omega(\alpha)} \right) \\ &=\; xy^k \left(f[0] + x \sum_{\alpha \neq 0} f[\alpha]\, x^{|\alpha|-1}y^{\omega(\alpha)} \right) \;=\; xy^k f[0] + x^2y^k \sum_{\alpha \neq 0} f[\alpha]\, x^{|\alpha|-1}y^{\omega(\alpha)} \end{aligned}$$

- As this is true for any $a \in A$ we have $xy^kA \subseteq xy^kE + x^2y^kB$. For the ideals $\mathfrak{a}_k$ we defined this turns into the following inclusion

$$\mathfrak{a}_k \;=\; \sum_{j=0}^{k} xy^jA \;\subseteq\; \sum_{j=0}^{k} xy^jE + \sum_{j=0}^{k} x^2y^jB \;\subseteq\; x\,\mathrm{Lh}_E\{\,1, y, \ldots, y^k\,\} + x^2B$$

 Form this we see that $xy^{k+1} \in \mathfrak{a}_{k+1}$ is not contained in $\mathfrak{a}_k$. As as the $\mathfrak{a}_k$ form an ascending chain, by construction, we conclude that this chain is strictly ascending

$$\mathfrak{a}_0 \;\subset\; \mathfrak{a}_1 \;\subset\; \ldots \;\subset\; \mathfrak{a}_k \;\subset\; \ldots$$

 Assume A was finitely generated, as E is a field (and hence noetherian) then (2.42) would tell us, that A is noetherian, too. But as we have the chain above, this is not the case. This proves, that A is not finitely generated - even though it is contained in the noetherian E-algebra B.

- Clearly $\{\, x, xy \,\}$ is algebraically independent: If $f \in E[s,t]$ is any polynomial, such that $f(x, xy) = 0$ then we get $f = 0$ from the fact, that $\{\, x, y \,\}$ is algebraically independent and we then have

$$0 \;=\; f(x, xy) \;=\; \sum_{\alpha \in \mathbb{N}^2} f[\alpha]\, x^{|\alpha|}y^{\alpha_2}$$

 Also any xy^k is algebraic over $E[x, xy]$: Just take the polynomial $g_k(t) := x^{k-1}t - (xy)^k$ then $g_k(xy^k) = x^ky^k - (xy)^k = 0$. But B is an integral domain and these elements generate A. Therefore the entire extension $A : E[x, xy]$ is algebraic, due to (8.41.(ii)).

- Let us now prove the proposition in two steps: First we assume $B := E[x]$ to be the polynomial ring in one variable. If $A = E$, then $A = E[0]$ is finitely generated, already, so let us suppose $E \subseteq A$. Then take

$$n \;:=\; \min\{\, \deg(a) \mid a \in A \setminus E \,\}$$

and let $p \in A$ be a monic polynomial with $\deg(p) = n$. Then $\varepsilon : E[t] \twoheadrightarrow E[p] : f \mapsto f(p)$ is surjective, by definition. But it also has $\mathrm{kn}(\varepsilon) = 0$, as $\deg(p) = n \geq 1$, by (7.27.(ii)) and hence is injective, too. That is $E[p]$ is isomorphic to a polynomial ring in one variable, under ε and hence a PID. As $p \in A \subseteq B$ we may regard A and $B = E[x]$ as $E[p]$-modules under multiplication as scalar multiplication. And by (8.29.(vi)) $R[x]$ has the basis $\{ 1, x, \ldots, x^{n-1} \}$ as an $E[p]$-module. In particular $B = E[x]$ is a free, finitely genrated $E[p]$-module, where $E[p]$ is a PID. Then by (3.104.(i)) the $E[p]$-sub-module $A \leq_{\mathfrak{m}} B$ is free and finitely generated, again. So let $\{ a_1, \ldots, a_m \}$ be a basis of A as an $E[p]$-module (where $m \leq n$), then we clearly have $A = \mathrm{Lh}_{E[p]}\{ a_1, \ldots, a_m \} \subseteq E[p, a_1, \ldots, a_m] \subseteq A$. That is A is finitely generated.

- Now consider a general $B = E[b]$, then we have an epimorphism of algebras $\varepsilon : E[x] \twoheadrightarrow B$ defined by $\varepsilon(f) = f(b)$. As $A \subseteq B$ is a sub-algebra, so is $A_0 := \varepsilon^{-1}(A) \subseteq E[x]$. As we have seen above, A_0 then is finitely generated, say $A_0 = E[a_1, \ldots, a_m]$ for some $a_i \in A_0$. As ε is surjective, we have $A = \varepsilon(\varepsilon^{-1}(A)) = \varepsilon(A_0)$ and as this is a homomorphism of E-algebras we conclude, that A is finitely generated, as well, since

$$A \;=\; \varepsilon(A_0) \;=\; \varepsilon\big(E[a_1, \ldots, a_m]\big) \;=\; E\big[\varepsilon(a_1), \ldots, \varepsilon(a_m)\big]$$

□

Proof of (8.33):
By (8.10(iii)) there is a finite ring extension $T : S$ such that the structural hohomorphism $\beta : S \hookrightarrow T$ is injective and p and q split over T. That is there are u_i and $v_j \in T$, such that

$$\begin{aligned} p(t) &= \prod_{i=1}^{m} (t - u_i) \\ q(t) &= \prod_{j=1}^{n} (t - v_j) \end{aligned}$$

By assumption both p and q are monic and hence pq is monic, too. Also we have $(pq)(u_i) = p(u_i)q(u_i) = 0 \cdot q(u_i) = 0$. That is $u_i \in T$ satisfies pq and in particular, it is integral over $\overline{R}$. Yet by (8.30.(vi)) this means that u_i already is integral over R: $u_i \in \mathrm{int}(T : R)$. But as $\mathrm{int}(T : R)$ is an intermediate ring of $T : R$ also any polynomial expression $f(u_1, \ldots, u_m)$ where $f \in R[t_1, \ldots, t_m]$ is integral over R. By the theorem of Vieta (7.66) the coefficients of p are elementary symmetric polynomials in the roots u_i and we have just argued, that these are integral over R again

$$p[k] \;=\; (-1)^{m-k} s^{(m)}_{m-k}(u_1, \ldots, u_m) \;\in\; \mathrm{int}(T : R)$$

for any $k \in 0 \ldots m$. In particular $p[k] \in \mathrm{int}(T : R) \cap S$ and hence $p[k] \in \mathrm{int}(S : R) = \overline{R}$. Altogether we have $p \in \overline{R}[t]$ and $q \in \overline{R}[t]$ follows in exactly the same manner. □

Proof of (8.37):
As $x \in S$ is integral over R, there is some monic polynomial $n \in R[t]$ with $n(x) = 0$. Let $E := \mathrm{quot}(R)$ be the quotient field of R and consider $R \subseteq E$ as a subset, canonically. Then the null ideal

$$\mathfrak{v}_x \;:=\; \{ h \in E[t] \mid h(x) = 0 \} \;\trianglelefteq_{\mathfrak{i}}\; E[t]$$

is non-zero, as $n \in \mathfrak{v}_x$. Yet $E[t]$ is a PID and hence we may take $m_x \in E[t]$ to be the monic generator of this ideal $\mathfrak{v}_x = m_x E[t]$. As $n \in m_x E[t]$ there is some $g \in E[t]$ such that $n = g m_x$. Recall that both n and m_x are monic and then g has to be monic, too [as $1 = \mathrm{lc}(n) = \mathrm{lc}(g) \cdot \mathrm{lc}(m_x) = \mathrm{lc}(g)$]. Thus by the lemma of Gauss (8.33) we have g, $m_x \in \overline{R}[t]$, where $\overline{R} = \mathrm{int}(E : R)$. But R is a normal domain, that is $\overline{R} = R$ and therefore $m_x \in R[t]$.
It remains to verify, that m_x is the minimal polynomial of x: We have (1) m_x is monic, by construction. And (2) $m_x(x) = 0$, as $m_x \in \mathfrak{v}_x$. (3) Let now $f(x) \in R[t]$ be any polynomial with $f(x) = 0$: If $f = 0$ then $f = 0 \cdot m_x$ and hence $m_x \mid f$ is clear. Otherwise take $a := \mathrm{lc}(f)$ and consider $h := (1/a)f \in E[t]$. Then $h(x) = 0$ as well and thereby $h = g\mu_x$ for some $g \in E[t]$. By the same reasoning as before (h and m_x are monic), we get $g(x) \in R[t]$. And thereby we get $f = ah = agm_x$ and $ag \in R[t]$. That is $m_x \mid f$ in $R[t]$, which is required for m_x to be the minimal polynomial. □

Proof of (8.32):

(i) Let us first prove the following statement: Given any prime ideal $\mathfrak{q} \trianglelefteq_{\mathrm{i}} S$ the pull-back $\Sigma(\mathfrak{q}) = \mathfrak{q} \cap R$ is a prime ideal of R again. Formally that is the implication

$$\mathfrak{q} \in \mathrm{Spec}(S) \quad \Longrightarrow \quad \mathfrak{q} \cap R \in \mathrm{Spec}(R)$$

First of all $\mathfrak{q} \cap R = \alpha^{-1}(\mathfrak{q})$ is an ideal again, as α is a homomorphism of rings. Also, if a, $b \in R$ with $ab \in \mathfrak{q} \cap R$ then we have $\alpha(a)\alpha(b) = \alpha(ab) \in \mathfrak{q}$. But as $\mathfrak{q}$ is prime we have $\alpha(a) \in \mathfrak{q}$ or $\alpha(b) \in \mathfrak{q}$. But this again is $a \in \mathfrak{q} \cap R$ or $b \in \mathfrak{q} \cap R$, such that $\mathfrak{q} \cap R$ is prime again. In particular Σ is well-defined.

(ii) Next we deal with the following statement: Given any maximal ideal $\mathfrak{n} \trianglelefteq_{\mathrm{i}} S$ the pull-back $\Sigma(\mathfrak{n}) = \mathfrak{n} \cap R$ is a maximal ideal of R again. Formally that is the implication

$$\mathfrak{n} \in \mathrm{Smax}(S) \quad \Longrightarrow \quad \mathfrak{n} \cap R \in \mathrm{Smax}(R)$$

To do this, let us abbreviate $\mathfrak{m} := \mathfrak{n} \cap R \trianglelefteq_{\mathrm{i}} R$. Then we regard the ring extension $S/\mathfrak{n}$ over $R/\mathfrak{m}$. As $S : R$ is integral (8.29.(ii)) tells us, that

$$S\Big/_{\mathfrak{n}} : R\Big/_{\mathfrak{m}} \text{ is integral}$$

too, under the injective structural homomorphism $\overline{\alpha} : a + \mathfrak{m} \mapsto \alpha(a) + \mathfrak{n}$. Now, as $\mathfrak{n}$ is maximal, $S/\mathfrak{n}$ is a field. But $\overline{\alpha}$ is injective such that $R/\mathfrak{m}$ is a field, as well, according to (8.30.(viii)). But this again means $\mathfrak{m} = \mathfrak{n} \cap R$ is maximal, as well. In particular the restriction of Σ to the maximal spectra is well-defined, as well.

(ii) Conversely let $\mathfrak{n} \in \mathrm{Spec}(S)$ be a prime ideal, such that $\mathfrak{m} := \mathfrak{n} \cap R$ is a maximal ideal. Then we need to show, that $\mathfrak{n}$ is a maximal ideal of S. Again we regard

$$S\Big/_{\mathfrak{n}} : R\Big/_{\mathfrak{m}} \text{ is integral}$$

As $\mathfrak{m}$ is maximal, $R/\mathfrak{m}$ is a field. But as $\mathfrak{n}$ was assumed to be prime, $S/\mathfrak{n}$ is an integral domain. So by (8.30.(viii)) again, we find $S/\mathfrak{n}$ to be a field. This in turn means, that $\mathfrak{n}$ is a maximal ideal.

(i) We are now able to prove, that (under the assumption that $S : R$ is integral) Σ is surjective. That is we are given any prime ideal $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ and need to find some prime ideal $\mathfrak{q} \trianglelefteq_{\mathrm{i}} S$, such that $\mathfrak{p} = \mathfrak{q} \cap R$. To do this let $U := R \setminus \mathfrak{p}$, which is multiplicatively closed, as $\mathfrak{p}$ is a prime ideal. As $S : R$ is integral (8.29.(iv)) tells us, that

$$U^{-1}S : U^{-1}R \text{ is integral}$$

too, under the structural isomorphism $U^{-1}\alpha(a) = a1_S/u$. Note that $U^{-1}R = R_{\mathfrak{p}}$ is a local ring with maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$ according to (2.138). We thereby obtain a commutative diagram of homomorphisms of rings

$$\begin{array}{ccccccccc} \kappa_R & : & R & \to & U^{-1}R & : & a & \mapsto & \frac{a}{1} \\ & & \downarrow & & \downarrow & & & & \\ \kappa_S & : & S & \to & U^{-1}S & : & s & \mapsto & \frac{s}{1} \end{array}$$

where the vertical maps are given by $\alpha : a \mapsto a1_S$ and $U^{-1}\alpha : a/1 \mapsto a1_S/1$ respectively. From this explicit description it is clear, that this diagram truly commutes. As $S \neq 0$ and $0 \notin U$ we have $U^{-1}S \neq 0$ and hence we can choose any maximal ideal $\mathfrak{u} \trianglelefteq_{\mathrm{i}} U^{-1}S$. Then by (ii) above, $\mathfrak{u} \cap U^{-1}R$ is a maximal ideal ideal of $U^{-1}R = R_{\mathfrak{p}}$. But as this ring is local it only has one maximal ideal, such that we find

$$\mathfrak{u} \cap U^{-1}R \;=\; \mathfrak{p}R_{\mathfrak{p}}$$

Let $\mathfrak{q} := \kappa_S^{-1}(\mathfrak{u}) \trianglelefteq_{\mathrm{i}} S$. As $\mathfrak{u}$ is a prime ideal (even a maximal ideal) $\mathfrak{q}$ is a prime ideal of R, by (i) above. It remains to prove, that $\mathfrak{q} \cap R = \mathfrak{p}$, which is reduced to the following computation:

$$\begin{aligned} \mathfrak{q} \cap R \;&=\; \alpha^{-1}(\mathfrak{q}) \;=\; \alpha^{-1}\big(\kappa_S^{-1}(\mathfrak{u})\big) \;=\; \big(\kappa_S\alpha\big)^{-1}(\mathfrak{u}) \;=\; \big(U^{-1}\alpha\,\kappa_R\big)^{-1}(\mathfrak{u}) \\ &=\; \kappa_R^{-1}\big(U^{-1}\alpha\big)^{-1}(\mathfrak{u}) \;=\; \kappa_R^{-1}\big(\mathfrak{u} \cap U^{-1}R\big) \;=\; \kappa_R^{-1}\big(\mathfrak{p}R_{\mathfrak{p}}\big) \;=\; \mathfrak{p}R_{\mathfrak{p}} \cap R \;=\; \mathfrak{p} \end{aligned}$$

(ii) But from this we find that the restriction of Σ to the maximal spectra is surjective, too: Consider any maximal ideal $\mathfrak{m}$ of R, in particular $\mathfrak{m}$ is prime and hence by the surjectivity (i) of Σ, there is some prime ideal $\mathfrak{n}$ of S, such that $\mathfrak{n} \cap R = \mathfrak{m}$. Now, as $\mathfrak{m}$ is maximal, we find that $\mathfrak{n}$ is maximal, too, by the second item (ii), so the restriction of Σ is surjective, as well.

(iii) Let us denote $\mathfrak{p} := \mathfrak{u} \cap R$, then by assumption we also have $\mathfrak{p} = \mathfrak{v} \cap R$. As $S : R$ is integral, so is $(S/\mathfrak{u}) : (R/\mathfrak{p})$ under the injective structural homomorphism $\overline{\alpha}(a + \mathfrak{p}) = \alpha(a) + \mathfrak{u}$, by (8.29.(iv)). And by the correspondence theorem (1.71) $\mathfrak{v}/\mathfrak{u}$ is an ideal of $R/\mathfrak{u}$. Let us evaluate its pull-back

$$\mathfrak{v}\Big/_{\mathfrak{u}} \cap R\Big/_{\mathfrak{p}} \;=\; \{\, a + \mathfrak{p} \mid \alpha(a) + \mathfrak{u} \in \mathfrak{v}/\mathfrak{u} \,\} \;=\; \{\, a + \mathfrak{p} \mid \alpha(a) \in \mathfrak{v} \,\} \;=\; \mathfrak{v} \cap R\Big/_{\mathfrak{p}}$$

As $\mathfrak{v} \cap R = \mathfrak{p}$, too we find that $\mathfrak{v}/\mathfrak{u} \cap R/\mathfrak{p} = 0$. So by (8.29.(ii)) the pull-back is contained in the set of zero-divisors $\mathfrak{v}/\mathfrak{u} \subseteq \mathrm{zd}(R/\mathfrak{p})$. Yet $\mathfrak{p}$ is a prime ideal by assumption and hence $R/\mathfrak{p}$ does not have any zero-divisors. And thereby we get $\mathfrak{u} = \mathfrak{v}$ from

$$\mathfrak{v}\Big/_{\mathfrak{u}} \cap R\Big/_{\mathfrak{p}} \;=\; \{\, 0 + \mathfrak{p} \,\}$$

(iv) Consider any ideal $\mathfrak{b} \trianglelefteq_{\mathrm{i}} S$ and let $\mathfrak{a} := \mathfrak{b} \cap R$. As $S : R$ is integral, (8.29.(ii)) once again tells us

$$S\big/_{\mathfrak{b}} : R\big/_{\mathfrak{a}} \text{ is integral}$$

under the injective structural homomorphism $\overline{\alpha} : a + \mathfrak{a} \mapsto \alpha(a) + \mathfrak{b}$. Thereby we get from (i), that $\overline{\Sigma} := \operatorname{Spec}(\overline{\alpha})$ is surjective. Now take a look at the following diagram

$$\begin{array}{rcccc} \overline{\Sigma} & : & \operatorname{Spec}(S/\mathfrak{b}) & \twoheadrightarrow & \operatorname{Spec}(R/\mathfrak{a}) \\ & & \updownarrow & & \updownarrow \\ \Sigma & : & \mathbb{V}(\mathfrak{b}) & \to & \mathbb{V}(\mathfrak{a}) \end{array}$$

where the vertical maps are $\mathfrak{q} \mapsto \mathfrak{q}/\mathfrak{b}$ and $\mathfrak{p} \mapsto \mathfrak{p}/\mathfrak{a}$ respectively. These are bijective, due to the correspondence theorem (1.71). And if $\mathfrak{q}$ is a prime ideal of S, with $\mathfrak{b} \subseteq \mathfrak{q}$, then it is clear that $\mathfrak{a} = \mathfrak{b} \cap R \subseteq \mathfrak{q} \cap R = \Sigma(\mathfrak{q})$. Hence the lower row of this diagram is well defined, too. This diagram is commutative, as we find

$$\begin{aligned} \overline{\Sigma}\left(\mathfrak{q}\big/_{\mathfrak{b}}\right) &= \overline{\alpha}^{-1}\left(\mathfrak{q}\big/_{\mathfrak{b}}\right) = \left\{ a + \mathfrak{a} \;\middle|\; \alpha(a) + \mathfrak{b} \in \mathfrak{q}\big/_{\mathfrak{b}} \right\} \\ &= \{\, a + \mathfrak{a} \mid \alpha(a) \in \mathfrak{q} \,\} = {}^{\alpha^{-1}(\mathfrak{q})}\big/_{\mathfrak{a}} = {}^{\Sigma(\mathfrak{q})}\big/_{\mathfrak{a}} \end{aligned}$$

But as this diagram commutes, $\overline{\Sigma}$ is surjective and the vertical maps even are bijective, we conclude that the bottom line $\Sigma : \mathbb{V}(\mathfrak{b}) \twoheadrightarrow \mathbb{V}(\mathfrak{a})$ is surjective, as well. And this is $\Sigma(\mathbb{V}(\mathfrak{b})) = \mathbb{V}(\mathfrak{a})$.

(v) If $\mathfrak{q} \in \Sigma^{-1}(\mathfrak{p})$, then $\mathfrak{p} = \Sigma(\mathfrak{q}) = \mathfrak{q} \cap R$. Then we get $\mathfrak{p}S = (\mathfrak{q} \cap R)S \subseteq \mathfrak{q}$ from (8.15). And as there is some $\mathfrak{q}$ with $\mathfrak{p} = \mathfrak{q} \cap R$ the same proposition implies $\mathfrak{p} = (\mathfrak{p}S) \cap R$. It remains to prove the minimality: Consider any prime ideal $\mathfrak{q}' \trianglelefteq_{\mathrm{i}} S$ such that $\mathfrak{p}S \subseteq \mathfrak{q}' \subseteq \mathfrak{q}$, then the pull-backs inherit these inclusions

$$\mathfrak{p} = (\mathfrak{p}S) \cap R \subseteq \mathfrak{q}' \cap R \subseteq \mathfrak{q} \cap R = \mathfrak{p}$$

such that $\mathfrak{q}' \cap R = \mathfrak{q} \cap R$ and $\mathfrak{q}' \subseteq \mathfrak{q}$. But according to (iii) this implies $\mathfrak{q}' = \mathfrak{q}$, as claimed.

(i) It remains to prove, that in case S is a noetherian ring, Σ has finite fibres only. We postponed this, as it requires (v): There we have seen that those $\mathfrak{q} \in \operatorname{Spec}(S)$ that satisfy $\mathfrak{q} \cap R = \mathfrak{p}$ are minimal over $\mathfrak{p}S$. But by (2.45.(iv)) $\mathbb{V}(\mathfrak{p}S)_*$ is a finite set and hence $\Sigma^{-1}(\mathfrak{q})$ is finite, too.

□

Proof of (8.51):

- Pick up the variables x_1 to x_n in another polynomial ring $E[x_1, \ldots, x_n]$. Then by (7.57.(iii)) there are some numbers $1 \leq m_2 \leq \cdots \leq m_n$ (that can be given explicitly) and some $a \in E$ with $a \neq 0$, such that the polynomial

$$ag\big(x_1, x_2 + x_1^{m_1}, \ldots, x_n + x_1^{m_n}\big) \in E[x_2, \ldots, x_n][x_1]$$

is monic, if we regard it, as a polynomial in x_1 over $E[x_2, \ldots, x_n]$. Suppose we are able, to prove the claims for $g_1 := ag$, then the claim remains true for general polynomials g: Let $b := a^{-1}$ such that $g = bg_1$. (1) If $\{\, g_1, z_2, \ldots, z_n \,\}$ is algebraically independent then $\{\, bg_1, z_2, \ldots, z_n \,\}$ is

algebraically independent, too, as $x_1 \mapsto bx_1$ and $x_i \mapsto x_i$ for $i \in 2 \dots n$ induces an automorphism on $E[x_1, \dots, x_n]$. (2) $E[bg_1, z_2, \dots, z_n] = E[g_1, z_2, \dots, z_n] = P$ such that this statement is unchanged. (3) Also $gP = g_1P$ and $gA = g_1P$, such that (3) is unchanged, too. Thus if we start with g_1 then the above is a monic polynomial, and hence we may assume $a = 1$, in the following.

- As in the claim, let us define $z_i := t_i - t_1^{m_i} \in A$ for any $i \in 2 \dots n$ (that is $t_i = z_i + t_1^{m_i}$) and consider the evaluation homomorphism $\varepsilon : E[x_1, \dots, x_n] \to A$, defined by $\varepsilon(x_1) := t_1$ and $\varepsilon(x_i) := z_i$ for $i \in 2 \dots n$. Then we get

$$\begin{aligned} \varepsilon\Big(g\big(x_1, x_2 + x_1^{m_1}, \dots, x_n + x_1^{m_n}\big)\Big) &= g\big(t_1, z_2 + t_1^{m_1}, \dots, z_n + t_1^{m_n}\big) \\ &= g\big(t_1, t_2, \dots, t_n\big) \;=\; g \;\in\; A \end{aligned}$$

 On the other hand this is a monic polynomial in t_1 over the ring $P_2 := E[z_2, \dots, z_n]$. Let us define $h_2(t) \in P_2[t]$ to be this polynomial in t, that is we denote

$$h_2(t) \;:=\; g\big(t, z_2 + t^{m_1}, \dots, z_n + t^{m_n}\big) \;\in\; P_2[t]$$

 Then we have just seen, that $h_2(t_1) = g$. Now define $z_1 := g \in A$ and $h(t) := h_2(t) - z_1 \in P[t]$, where $P := E[z_1, z_2, \dots, z_n]$. Then by construction we have

$$h(t_1) \;=\; h_2(t_1) - z_1 \;=\; g - g \;=\; 0$$

- Note that h still is a monic polynomial in t over P, that satisfies $h(t_1) = 0$. Its leading term is of degree $\deg(h_2) = \deg_1(g) + m_2\deg_2(g) + \dots + m_n\deg_n(g)$ and as $\deg(g) \geq 1$ this means $\deg(h) \geq 1$, as well [note, that $g \in P[t]$ is a constant polynomial, as $g \in P$]. That is $h \neq 0$ and hence $t_1 \in A$ is integral over P. Therefore $P[t_1] : P$ is an integral extension, by (8.30) (i) and (iii). As we clearly have $t_1 \in P[t_1]$ and for any $i \in 2 \dots n$ also $t_i = z_i + t_1^{m_i} \in P[t_1]$, we find $A = E[t_1, \dots, t_n] \subseteq P[t_1] \subseteq A$, that is $P[t_1] = A$. We conclude, that $A : P = P[t_1] : P$ is integral and finitely generated (by t_1 only. That is $A : P$ is a finite extension, by (8.30.(v)).

- Now by (8.49.(iii)) we have $\operatorname{trdeg}(A : E) = \operatorname{trdeg}(A : P) + \operatorname{trdeg}(P : E)$. Hereby $\operatorname{trdeg}(A : E) = n$, as $\{ t_1, \dots, t_n \}$ is a transcendence basis of $A : E$ and $\operatorname{trdeg}(A : P) = 0$ as this is an algebraic extension - refer to example (8.48). So this leaves us with $\operatorname{trdeg}(P : E) = n$ and we recall $P = E[z_1, z_2, \dots, z_n]$. As $\{ z_1, \dots, z_n \}$ algebraically generates P there is a subset $V \subseteq \{ z_1, \dots, z_n \}$ that is a transcendence basis of $P : E$ - this is (8.47.(i)) for $U = \emptyset$ and $W = \{ z_1, \dots, z_n \}$. But $\#V = \operatorname{trdeg}(P : E) = n = \#W$ such that $V = \{ z_1, \dots, z_n \}$ already was a transcendence basis, to begin with. Thus we have proved parts (1) and (2).

- Therefore $P = E[z_1, \dots, z_n]$ is isomorphic (as an E-algebra) to a polynomial ring $R = E[x_1, \dots, x_n]$ in n variables, where the isomorphism is induced by $x_i \mapsto z_i$ - refer to (8.46.(i)). But as $x_1R \trianglelefteq_{\mathfrak{i}} R$ is a prime ideal, this implies, that $z_1P \trianglelefteq_{\mathfrak{i}} P$ is a prime ideal, too. Recall that $A : P$ is integral. Hence by the lying-over-theorem (8.32.(i)) there is a prime ideal $\mathfrak{u} \trianglelefteq_{\mathfrak{i}} A$ such that

$$z_1P \;=\; \mathfrak{u} \cap P$$

 We now want to prove $z_1P = gA \cap P$, as $z_1 = g$ and we still need to finish part (2) of the claim.

As $z_1 = g \in gA$ and $z_1 \in P$ we clearly have $z_1 \in gA \cap P$ and thereby $z_1P \subseteq gA \cap P$, as $gA \cap P$ is an ideal of P. It remains to verify the converse inclusion $gA \cap P \subseteq z_1P$: We get $z_1A \subseteq \mathfrak{u}$ from $z_1A = (z_1P)A = (\mathfrak{u} \cap P)A \subseteq \mathfrak{u}$, which are true in any ring-extension, according to (8.15) and (8.18). And from this inclusion we also get $gA \cap P = z_1A \cap P \subseteq \mathfrak{u} \cap P = z_1P$. Altogether we have $gP = z_1P = gA \cap P$, which has been claimed, in (3).

□

Proof of (8.52):

- **Claim 1:** Let $(E, +, \cdot)$ be a field and $A := E[t_1, \ldots, t_n]$ be the polynomial ring in $n \in \mathbb{N}$ variables. Also let $\mathfrak{a} \trianglelefteq_{\mathrm{i}} A$ be a proper ideal $\mathfrak{a} \neq A$. Then there is $\{ z_1, \ldots, z_n \} \subseteq A$ an algebraically independent set and some $k \in 0 \ldots n$ such that for $P := E[z_1, \ldots, z_n]$ we get $A : P$ is finite and

$$\mathfrak{a} \cap P \quad = \quad z_1P + \cdots + z_kP$$

- Nota the proof is very technical, so let us give a sketch of what we are about to do: We start with some $g_1 \in \mathfrak{a}$, $g_1 \neq 0$ and find a transcendence basis $\{ g_1, z_1, \ldots, z_n \}$. Then we iterate (induction on n), choose $g_2 \in \mathfrak{a} \cap E[z_2, \ldots, z_n]$ with $g_2 \neq 0$ and find a transcendence basis $\{ g_2, y_3, \ldots, y_n \}$. Then $\{ g_1, g_2, y_3, \ldots, y_n \}$ is a transcendence basis of $A : E$ again. We will go on, that is pick $g_3 \in \mathfrak{a} \cap E[y_3, \ldots y_n]$ with $g_3 \neq 0$ and so on, until - at some point - $\mathfrak{a} \cap E[x_j, \ldots, x_n] = 0$, then we stop an let $k = n - j$. The notation will be a little different, however.

- **Proof of 1:** If $n = 0$, then $A = E$ and hence $\emptyset$ is a transcendence basis of $A : E$. In this case $P = E[\emptyset] = E = A$ and hence $[A : P] = 1$ is finite. The only proper ideal of $A = E$ is $\mathfrak{a} = 0$ and therefore $\mathfrak{a} \cap P = 0$, such that $k = 0$ does the trick. Thus $n = 0$ is just a weird special case.

 If $\mathfrak{a} = 0$, then we can take $z_i := t_i$ and $k := 0$. Then $P = E[t_1, \ldots, t_n] = A$ and $\mathfrak{a} \cap P = 0$, so (1) and (2) are satisfied trivially and $\mathfrak{a} \cap P = 0$ also is property (3). So in the following let us only consider the case $n \geq 1$ and $\mathfrak{a} \neq 0$:

- We will do this by induction on n: In case $n = 1$ we have $A = E[t_1]$, which is a PID. Hence $\mathfrak{a}$ is of the form $\mathfrak{a} = gA$ for some $g \neq 0$ and therefore we can invoke (8.51) to find $z_1 = g$ and $k = 1$. So let us commence with the induction step $n \geq 2$:

 Choose any $g \in \mathfrak{a}$ with $g \neq 0$. Then by (8.51) there is $\{ g, z_2, \ldots, z_n \} \subseteq A$ an algebraically independent set such that for $Z := E[g, z_2, \ldots, z_n]$ we have: $A : Z$ is a finite ring-extension and $gZ = gA \cap Z$. Now let $Z_0 := E[z_2, \ldots, z_n]$ and

$$\mathfrak{a}_0 \quad := \quad \mathfrak{a} \cap Z_0$$

 As $\{ z_2, \ldots, z_n \}$ is algebraically independent, as it is a subset of such a set. Therefore we have an isomorphism of from the polynomial ring $E[x_2, \ldots, x_n] \xrightarrow{\sim} Z_0$ induced by $x_i \mapsto z_i$. Hence we can apply the induction hypothesis to $\mathfrak{a}_0 \trianglelefteq_{\mathrm{i}} Z_0$ [to be precise we apply it to the isomorphic copy of $\mathfrak{a}_0$ in $E[x_2, \ldots, x_n]$ and transfer the result back into Z_0]. That is we find an algebraically independent

set $\{ y_2, \ldots, y_n \} \subseteq Z_0$ such that $Z_0 : Y_0$ is finite, where $Y_0 := E[y_2, \ldots, y_n]$. Also there is some $k \in 0 \ldots n$ such that for we have

$$\mathfrak{a}_0 \cap Y_0 \;=\; y_2 Y_0 + \cdots + y_k Y_0$$

- Let us summarize: (1) A is an integral domain, (2) $\{ g, z_2, \ldots, z_n \}$ is a transcendence basis of $A : E$, (3) $\{ y_2, \ldots, y_n \}$ is algebraically independent, (4) $Y_0 \subseteq Z_0$ and (5) $Z_0 : Y_0$ is finite and hence algebraic. That is all the requirements of the basis exchange theorem (8.46.(vi)) are satisfied and this makes $\{ g, y_2, \ldots, y_n \}$ another transcendence basis of $A : E$.

- Let $Y := E[g, y_2, \ldots, y_n]$ then we need to show, that $A : Y$ even is finite: By construction we have $Z = E[g, z_2, \ldots, z_n] = Y[z_2, \ldots, z_n]$. For one g is integral over Y, as even $g \in Y$. Now recall that $Z_0 : Y_0$ finite, and hence integral. In particular any z_i is integral over Y_0 and thereby over Y, too. Thus Z is finitely generated by integral elements over Y and hence finite $[Z : Y] < \infty$ by (8.30.(ii)). But $A : Z$ is finite, as well and hence we find, that $A : Y$ is finite by (8.7.(iv))

$$[A : Y] \;\leq\; [A : Z] \cdot [Z : Y] \;<\; \infty$$

- Y will take the role of P in the claim and we want to prove, that the algebraically independent set $\{ g, y_2, \ldots, y_n \} \subseteq A$ also satisfies the identity of $\mathfrak{a} \cap P$. By now we have $\mathfrak{a}_0 \cap Y_0 = y_2 Y_0 + \cdots + y_k Y_0$ and $\mathfrak{a} \cap Z = gA \cap Z$ and remains to prove

$$\mathfrak{a} \cap Y \;=\; gY + y_2 Y + \cdots + y_n Y$$

 We start with the inclusion from right to left. As $g \in \mathfrak{a}$ and $g \in Y$ we find $gY \subseteq \mathfrak{a} \cap Y$. Also, for any $i \in 2 \ldots n$ we have $y_i \in y_2 Y_0 + \cdots + y_n Y_0 = \mathfrak{a}_0 \cap Y_0 = \mathfrak{a} \cap Z_0 \cap Y_0 = \mathfrak{a} \cap Y_0 \subseteq \mathfrak{a} \cap Y$. As g and any y_i are contained in $\mathfrak{a} \cap Y$ and this is an ideal, we have $gY + y_2 Y + \cdots + y_n Y \subseteq \mathfrak{a} \cap Y$.

- For the converse inclusion we regard some $f \in \mathfrak{a} \cap Y$. For systematic reasons let $y_1 := g$ and write f as a polynomial in y_1 over Y_0

$$f \;=\; \sum_{k=0}^{d} f_k(y_2, \ldots, y_n)\, y_1^k \;\in\; Y_0[y_1]$$

 For $k \geq 1$ we can pull put one $y_1 = g$ and hence find a term gp (where p is the term in brackets, below) that is an element of Y. As $g \in \mathfrak{a}$ we also see that gp is contained in $\mathfrak{a}$ and hence $gp \in \mathfrak{a} \cap Y$

$$f \;=\; f_0(y_2, \ldots, y_n) + g \left(\sum_{k=1}^{d} f_k(y_2, \ldots, y_n)\, y_1^{k-1} \right)$$

 That is we have $f = f_0 + gp$, where $p \in Y$ and hence $gp \in \mathfrak{a} \cap Y$, as we have argued above. Also $f \in \mathfrak{a}$ such that $f_0(y_2, \ldots, y_n) = f - gp \in \mathfrak{a}$, too. Also $f_0(y_2, \ldots, y_n) \in Y_0$ such that we get $f_0(y_2, \ldots, y_n) \in \mathfrak{a} \cap Y_0 = y_2 Y_0 + \cdots + y_n Y_0$. Altogether that is f is contained in

$$f \;=\; f_0(y_2, \ldots, y_n) + gp \;\in\; y_2 Y_0 + \cdots + y_n Y_0 + gY$$

In particular $\mathfrak{a} \cap Y \subseteq gY + y_2Y + \cdots + y_nY$ such that we have the equality. Hence the induction step is completed: We have proved (1) that $\{ g, y_2, \ldots, y_2 \}$ is a transcendence basis of $A : E$ and (2) the identity above, for $\mathfrak{a} \cap Y$, where $Y = E[g, y_2, \ldots, y_n]$.

- **Claim 2:** Let $(E, +, \cdot)$ be a field and $A = E[t_1, \ldots, t_n]$ be the polynomial ring in $n \in \mathbb{N}$ variables. Also consider a chain $\mathfrak{a} \subseteq \mathfrak{a}_2 \subseteq \ldots \subseteq \mathfrak{a}_r \trianglelefteq_{\mathrm{i}} A$ of proper ideals in A, that is $\mathfrak{a}_r \neq A$, of length $r \in \mathbb{N}$. Then there are a set of algebraically independent elements $\{ z_1, \ldots, z_n \} \subseteq A$ and increasing numbers $0 \leq k(1) \leq k(2) \leq \cdots \leq k(r) \leq n$ such that $A : P$ is a finite ring-extension, where $P := E[z_1, \ldots, z_n]$, and for any $i \in 1 \ldots r$ we have the identity

$$\mathfrak{a}_i \cap P \;=\; z_1P + \cdots + z_{k(i)}P$$

- **Proof of 2:** This time, we use induction on r. If $r = 0$, then the claim is trivial: $\{ t_1, \ldots, t_n \} \subseteq A$ is algebraically independent and $A = E[t_1, \ldots, t_n]$ and that's all. The case $r = 1$ is claim 1 exactly, so we only need to regard $r \geq 2$: By induction hypothesis we have an algebraically independent set $\{ y_1, \ldots, y_n \} \subseteq A$ and some numbers $0 \leq k(1) \leq \cdots \leq k(r-1) \leq n$ such that $A : R$ is finite and for any $i \in 1 \ldots (r-1)$ we have

$$\mathfrak{a}_i \cap R \;=\; y_1R + \cdots + y_{k(i)}R$$

 where $R := E[y_1, \ldots, y_n]$. Now abbreviate $h := k(r-1)$, $Q := E[y_{h+1}, \ldots, y_n]$ and $\mathfrak{b} := \mathfrak{a}_r \cap Q$. As before Q is isomorphic to a polynomial ring $E[x_{h+1}, \ldots, x_n]$, as $\{ y_{h+1}, \ldots, y_n \}$ is algebraically independent, as the larger set $\{ y_1, \ldots, y_n \}$ is so, too. Therefore we can use claim 1 on $\mathfrak{b} \trianglelefteq_{\mathrm{i}} Q$ to find an algebraically independent set $\{ z_{h+1}, \ldots, z_n \} \subseteq Q$ and some $k \in h \ldots n$ such that $Q : P$ is finite, where $P := E[z_{h+1}, \ldots, z_n]$ we have

$$\mathfrak{a}_r \cap P \;=\; \mathfrak{b} \cap P \;=\; z_{h+1}P + \cdots + z_kP$$

 Recall, that (1) A is an integral domain, (2) $V := \{ y_1, \ldots, y_n \}$ is a transcendence basis of $A : E$, (3) $U' := \{ z_{h+1}, \ldots, z_n \}$ is algebraically independent, (4) for $P = E[U']$ and $Q = E[U]$ with $U := \{ y_{h+1}, \ldots, y_n \} \subseteq V$ we have $P \subseteq Q$ and (5) $Q : P$ is algebraic, as it even is a finite ring-extension. That is all the requirements of the basis exchange theorem (8.46.(iv)) are met and hence $(V \setminus U) \cup U' = \{ y_1, \ldots, y_h, z_{h+1}, \ldots, z_n \}$ is a transcendence basis of $A : E$, too.

- Now denote $R' := R[y_1, \ldots, y_h, z_{h+1}, \ldots, z_n] = P[y_1, \ldots, y_h]$. This will take the role of P in the claim, so we need to show that $A : R'$ is a finite ring-extension. The idea is the same, as in claim 1 before: We already know, that $A : R$ is finite, so let us prove, that $R : R'$ is finite, too: Note that by construction we have $R = R'[y_{h+1}, \ldots, y_n]$. Also for $h + 1 \leq j \leq n$ we have $y_j \in Q$ and $Q : P$ is finite. Hence y_j is integral over P (8.30.(iii)) and as $P \subseteq R'$ also over R'. That is R is generated by finitely many integral elements (y_j where $h + 1 \leq j \leq n$) and hence finite (8.30.(ii)). Then $A : R'$ is finite, as $[A : R'] \leq [A : R] \cdot [R : R'] < \infty$ ((8.7.(iv))).

- As we have found our candidate $\{ y_1, \ldots, y_h, z_{h+1}, \ldots, z_n \}$ for an algebraically independent set and already have $A : R'$ finite, it remains to prove that the identities for $\mathfrak{a}_i \cap R'$ are satisfied, for any $i \in 1 \ldots r$. Let us first consider $i \in 1 \ldots r-1$, the case $i = r$ will be the next step. Then we have

to prove

$$\mathfrak{a}_i \cap R' \;=\; y_1 R' + \cdots + y_{k(i)} R'$$

Consider any $j \in 1 \ldots k(i)$, then $y_j \in y_j R \subseteq \mathfrak{a}_i \cap R$ by the induction hypothesis (see above). That is $y_j \in \mathfrak{a}_i$. Also $y_j \in R'$ as $j \leq k(i) \leq k(r-1) = h$ by construction. That is we have $y_j \in \mathfrak{a}_i \cap R'$ and as this is true for any $j \leq k(i)$ we conclude

$$\mathfrak{a}_i \cap R' \quad \supseteq \quad y_1 P' + \cdots + y_{k(i)} R'$$

Conversely consider any $f \in \mathfrak{a}_i \cap R'$. Let us consider f as an element of the polynomial ring $f \in R' = E[y_1, \ldots, y_{k(i)}][x_{k(i)+1}, \ldots, x_n]$ where $x_j = y_j$ for $k(i) < j \leq h$ and $x_j = z_j$ for $h < j \leq n$ respectively. Then we can split f into

$$f \;=\; \sum_{\alpha \in \mathbb{N}^{k(i)}} \sum_{\beta \in \mathbb{N}^{n-k(i)}} f[\alpha, \beta]\, y^\alpha x^\beta \;=\; \sum_{\alpha \in \mathbb{N}^{k(i)}} \left(\sum_{\beta \in \mathbb{N}^{n-k(i)}} f[\alpha, \beta]\, x^\beta \right) y^\alpha$$

Thereby the terms in brackets $f_\alpha := \sum_\beta f[\alpha, \beta] x^\beta$ are contained in $E[x_{k(i)+1}, \ldots, x_n] \subseteq R'$. That is for any $j \in 1 \ldots k(i)$ we have $\deg_j(f_\alpha) = 0$ (or even $f_\alpha = 0$). Let us now spit this sum into $\alpha = 0$ and those $\alpha \in \mathbb{N}^{k(i)}$ with $\alpha \neq 0$

$$f \;=\; f_0 + \sum_{\alpha \neq 0} f_\alpha\, y^\alpha$$

If $\alpha \neq 0$ there is some $j \in 1 \ldots k(i)$ such that $\alpha_j \geq 1$. Hence we have $y_j \mid y^\alpha$ for this j. And altogether we find that the latter part $g = f - f_0$ is contained in

$$g \;:=\; \sum_{\alpha \neq 0} f_\alpha\, y^\alpha \;\in\; y_1 R' + \cdots + y_{k(i)} R'$$

As also any $y_j \in \mathfrak{a}_i$ by the inclusion, we already proved, we find $g \in \mathfrak{a}_i$, as well. But $f \in \mathfrak{a}_i$ is true by assumption, so we have $f_0 = f - g \in \mathfrak{a}_i$. Also $f_0 \in R' \subseteq R$ such that $f_0 \in \mathfrak{a}_i \cap R = y_1 R + \cdots + y_{k(i)} R$. Thus we either have $f_0 = 0$ or $\deg_j(f_0) \geq 1$ for some $j \in 1 \ldots k(i)$. But by construction of f_0 as an element of $f_0 \in E[x_{k(i)+1}, \ldots, x_n]$ we have $\deg_j(f_0) = 0$ for any $j \in 1 \ldots k(i)$ such that $f_0 = 0$ is the only viable possibility. That is $f = g$ and hence

$$f \;=\; \sum_{\alpha \neq 0} f_\alpha y^\alpha \;\in\; y_1 R' + \cdots + y_{k(i)} R'$$

- It remains to prove the identity of $\mathfrak{a}_r \cap R'$. Due to the very technical construction in which the transcendence basis $\{ y_1, \ldots, y_h, z_{h+1}, \ldots, z_n \}$ of $A : E$ features elements of different names, we have to prove the identity

$$\mathfrak{a}_r \cap R' \;=\; y_1 R' + \cdots + y_h R' + z_{h+1} R' + \ldots z_k R'$$

That is we took $k(r) := k \geq h = k(r-1)$. For $j \in 1 \ldots h$ we have $y_j \in \mathfrak{a}_{r-1} \subseteq \mathfrak{a}_r$ and $y_j \in R'$, as well such that $y_j R' \subseteq \mathfrak{a}_r \cap R'$. And for any $j \in h+1 \ldots k$ we have $z_j \in z_j P \subseteq \mathfrak{a}_r \cap P \subseteq \mathfrak{a}_r$ such

that $z_j \in \mathfrak{a}_r$ and $z_j \in R'$ make $z_j R' \subseteq \mathfrak{a}_r \cap R'$. Therefore we have the inclusion

$$\mathfrak{a}_r \cap R' \quad \supseteq \quad y_1 R' + \cdots + y_h R' + z_{h+1} R' + \ldots z_k R'$$

Conversely regard any $f \in \mathfrak{a}_r \cap R'$ again. As $R' = E[z_{h+1}, \ldots, z_n][y_1, \ldots, y_h]$ we decompose f (as above) according to this structure of R'. That is we write f as

$$f \;=\; \sum_{\alpha \in \mathbb{N}^h} \sum_{\beta \in \mathbb{N}^{n-h}} f[\alpha, \beta]\, y^\alpha z^\beta \;=\; \sum_{\alpha \in \mathbb{N}^h} \left(\sum_{\beta \in \mathbb{N}^{n-h}} f[\alpha, \beta]\, z^\beta \right) y^\alpha$$

Hereby $f_\alpha := \sum_\beta f[\alpha, \beta]\, z^\beta \in P$ as $P = E[z_{h+1}, \ldots, z_n]$. Again we split f into the component f_0 for $\alpha = 0$ and the rest g which contains all summands with $\alpha \neq 0$

$$f \;=\; f_0 + \sum_{\alpha \neq 0} f_\alpha\, y^\alpha$$

If $\alpha \neq 0$ then for some $j \in 1 \ldots h$ we have $\alpha_j \geq 1$ and therefore $y_j \mid y^\alpha$. That is $f_\alpha y^\alpha$ is contained in $y_1 P + \cdots + y_h P$ and in particular in $y_1 R' + \ldots y_h R'$. It remains to deal with f_0: As $g := f - f_0 \in y_1 R' + \ldots y_h R' \subseteq \mathfrak{a}_r \cap R' \subseteq \mathfrak{a}_r$ has already been proved, we have both $g \in \mathfrak{a}_r$ and $f \in \mathfrak{a}_r$ such that $f_0 = f - g \in \mathfrak{a}_r$ too. As $f_0 \in P$ by construction, we have $f_0 \in \mathfrak{a}_r \cap P = z_{h+1} P + \cdots + z_k P$, in particular $f_0 \in z_{h+1} R' + \cdots + z_k R'$. Therefore we have also found the converse inclusion, as

$$f \;=\; f_0 + g \;\in\; z_{h+1} R' + \cdots + z_k R' + y_1 R' + \ldots y_h R'$$

- **Claim 3:** The Noetherian Normalisation Theorem itself. That is we drop the restriction of A being a polynomial ring $A = E[t_1, \ldots, t_n]$ and consider any finitely generated E-algebra $A \neq 0$.

- **Proof of 3:** By assumption A is finitely generated, say $A = E[x_1, \ldots, x_m]$ for some $x_i \in A$. Then clearly we have an epimorphism of E-algebras from the polynomial ring $E[t_1, \ldots, t_m]$ onto A, induced by evaluating $t_i \mapsto x_i$

$$\pi \,:\, E[t_1, \ldots, t_m] \;\twoheadrightarrow\; A \,:\, t_i \mapsto x_i$$

Let $\mathfrak{b}_0 := \mathrm{kn}(\pi)$ and for any $i \in 1 \ldots r$ also $\mathfrak{b}_i := \pi^{-1}(\mathfrak{a}_i)$. Then $\mathfrak{b}_0 \subseteq \mathfrak{b}_1 \subseteq \ldots \mathfrak{b}_r$ is an ascending chain of ideals in $B := E[t_1, \ldots, t_m]$. Not much of a surprise: We use claim 2 on B with this chain of ideals. That is there are algebraically independent elements $\{ q_1, \ldots, q_m \} \subseteq B$ and numbers $0 \leq l(0) \leq l(1) \leq \cdots \leq l(r) \leq m$ such that $B : Q$ is finite, where $Q := E[q_1, \ldots, q_m] \subseteq B$ and for any $i \in 0 \ldots r$ we get

$$\mathfrak{b}_i \cap Q \;=\; q_1 Q + \cdots + q_{l(i)} Q$$

Now let $n := m - l(0)$ and for any $i \in 1 \ldots r$ also $k(i) := l(i) - l(0)$. For any $j \in 1 \ldots n$ also take $p_j := \pi(q_{j+l(0)}) \in A$ and $P := E[p_1, \ldots, p_n] \subseteq A$.

- For $j \leq l(0)$ we have $q_i \in q_i Q \subseteq \mathfrak{b}_0 = \mathrm{kn}(\pi)$ and hence $\pi(q_j) = 0$. And for $j > l(0)$ we have $\pi(q_j) = p_{j-l(0)} \in P$. As all p_i are covered $[q_{1+l(0)} \mapsto p_1$ until $q_m \mapsto q_n]$ we find $\pi(Q) = P$. Recall that $B : Q$ is finite $\pi : B \twoheadrightarrow A$ is surjective and as we have just seen $\pi(Q) = P$. Then (8.28) tells

us, that $A : P$ is a finite ring-extension, too.

- We will now prove, that $\pi : E[q_{1+l(0)}, \ldots, q_n] \to E[p_1, \ldots, p_n]$ is an isomorphism: The surjectivity is clear, as $q_{j+l(0)} \mapsto p_j$ and the p_j generate P. For the injectivity we first note, that

$$\mathrm{kn}(\pi) \cap Q \;=\; \mathfrak{b}_0 \;=\; q_1 Q + \cdots + q_{l(0)} Q \;\subseteq\; E[q_1, \ldots, q_{l(0)}]$$

 Thus if $q \in E[q_{1+l(0)}, \ldots, q_n]$ with $\pi(q) = 0$ then we have $q \in E[q_1, \ldots, q_{l(0)}]$, as well. The only elements that are contained in both sets are scalars $q \in E$. But then $0 = \pi(q) = q\pi(1_B) = q1_A$, as π is an E-algebra homomorphism. But E is a field and $A \neq 0$, by assumption. Thus we have $q = 0$ and therefore π is injective, when restricted to $E[q_{1+l(0)}, \ldots, q_n]$. As the elements $\{ q_1, \ldots, q_m \}$ are algebraically independent we see, that $\{ p_1, \ldots, p_n \}$ are algebraically independent, too, as any (polynomial) relation between them could be pulled back to a (polynomial) relation of the $\left\{ q_{1+l(0)}, \ldots, q_n \right\}$. But as this set is algebraically independent, there is no such relation.

- It remains to verify the identity for the ideals $\mathfrak{a}_i \cap P$. Recall that $\mathfrak{b}_i = \pi^{-1}(\mathfrak{a}_i) = \{ b \in B \mid \pi(b) \in \mathfrak{a}_i \}$ and for any $i \in 1 \ldots r$ we have $\mathfrak{b}_i \cap Q = q_1 Q + \cdots + q_{l(i)} Q$. We now have to verity

$$\mathfrak{a}_i \cap P \;=\; p_1 P + \cdots + p_{k(i)} P$$

 We now claim $\pi(\mathfrak{b}_i \cap Q) \subseteq \mathfrak{a}_i \cap P$: That is we regard some $q \in \mathfrak{b}_i \cap Q$. As $q \in \mathfrak{b}_i = \pi^{-1}(\mathfrak{a}_i)$ we have $\pi(q) \in \mathfrak{a}_i$. Also $q \in Q$ turns into $\pi(q) \in \pi(Q) = P$. That is $\pi(q) \in \mathfrak{a}_i \cap P$ and so we are done. Conversely $\pi(\mathfrak{b}_i \cap Q) \supseteq \mathfrak{a}_i \cap P$ is true as well: We start with any $p \in \mathfrak{a}_i \cap P$. As $\pi(Q) = P$, there is some $q \in Q$ with $\pi(q) = p$. Also we get $q \in \pi^{-1}(\mathfrak{a}_i) = \mathfrak{b}_i$ by construction. Thus we have $q \in \mathfrak{p}_i \cap Q$ and therefore $p = \pi(q) \in \pi(\mathfrak{p}_i \cap Q)$. Altogether we have

$$\pi\big(\mathfrak{b}_i \cap Q\big) \;=\; \mathfrak{a}_i \cap P$$

 But we also have $\pi(q_j) = 0$ for $1 \leq j \leq l(0)$ and $\pi(q_j) = p_{j-l(0)}$ for $l(0) < j < m$. And as also $\pi(Q) = P$ we find the identity for $\mathfrak{a}_i \cap P$ by an easy computation

$$\mathfrak{a}_i \cap P \;=\; \pi\big(\mathfrak{b}_i \cap Q\big) \;=\; \pi\left(\sum_{j=1}^{l(i)} q_j Q\right) \;=\; \sum_{j=1}^{l(i)} \pi\big(q_j\big) P \;=\; \sum_{j=l(0)+1}^{l(i)} p_{j-l(0)} P \;=\; \sum_{j=1}^{l(i)-l(0)} p_j P$$

 Recall that $k(i) = l(i) - l(0)$ such that we truly have $\mathfrak{a}_i \cap P = p_1 P + \cdots + p_{k(i)} P$. This is property (3) of the claim. We already have (1), that $\{ p_1, \ldots, p_n \}$ is algebraically independent and (2) that $A : P$ is finite. We are done, at long last.

□

Proof of (8.55):

- All the proofs are astoundingly simple, all we have to do is reap the harvest from previous propositions: For (b) $\implies$ (c) for example it suffices to note, that any finite extension $K : F$ already is algebraic, according to (8.30.(iii)). For (c) $\implies$ (a) we pick up any $z \in K$, that is algebraic over F. As F is a field z is integral over F. Then $F[z] : F$ is finite, by (8.30.(i)) such that $F[z] = F1_K$, by assumption. But this means $\mathrm{alg}(K : F) \subseteq F1_K$ and the converse inclusion is clear.

- Let us continue with (c) $\implies$ (d): As $\deg(f) \geq 1$ we can invoke (8.10.(iv)) to bring up a field K, such that $K : F$ is finite and f splits over K. That is f is of the form

$$f(t) \;=\; a\prod_{i=1}^{n}(t - z_i)$$

for some $z_i \in K$, where the identity is in $K[t]$. Thereby we see $n = \deg(f)$ by comparing the degrees of these terms. As $K : F$ is finite, assumption (c) tells us that $z_i = x_i 1_K$ for some $x_i \in F$. As $\alpha : F \hookrightarrow K : a \mapsto a1_k$ is injective, this also implies the following identity in $F[t]$

$$f(t) \;=\; a\prod_{i=1}^{n}(t - x_i)$$

- The implication (d) $\implies$ (e) is clear, just choose $x = x_1$ as a root. For (e) $\implies$ (f) we choose any $x \in F$ such that $p(x) = 0$. From this we get $t - x \mid p$, according to (7.54.(iii)). But as p is irreducible and $t - x$ is not a unit in $E[t]$, this means $p = a(t - x)$ for some $E[t]^* = E^*$. In particular $\deg(p) = 1$. This enables us to also prove (f) $\implies$ (a): Choose any $z \in \mathrm{alg}(K : F)$, as z is algebraic and F is a field (hence an UFD, hence normal), z admits a minimal polynomial m_x, according to (8.37). But $p := m_x$ is prime and hence irreducible. Thus by assumption (f) we have $\deg(m_x) = 1$. This means $m_x = t - a$ for some $a \in F$. But as $0 = m_x(x) = x - a1_K$ this implies $x = a1_K \in F1_K$. As this is true for any z we get $\mathrm{alg}(K : F) \subseteq F1_K$ and the converse implication is clear, again.

□

Proof of (8.56):
If $\mathfrak{m} \trianglelefteq_{\mathrm{i}} F[t]$ is a maximal ideal, then $\mathfrak{m} = pF[t]$ for some $p \in F[t]$, as $F[t]$ is an euclidean domain and hence a PID. And as any maximal ideal is prime, p is prime and hence irreducible. Conversely, if $p \in F[t]$ is irreducible, then choose a maximal ideal $\mathfrak{m}$ such that $pF[t] \subseteq \mathfrak{m}$. Choose $m \in F[t]$ such that $\mathfrak{m} = mF[t]$, then $pF[t] \subseteq mF[t]$ implies $m \mid p$. That is $p = mf$ for some $f \in F[t]$. As p is irreducible, we have m or $f \in F[t]^*$. If we had $m \in F[t]^*$ then $\mathfrak{m}$ would be the whole ring $F[t]$, in contradiction to $\mathfrak{m}$ being maximal. Thus we have $f \in F[t]^*$ and thereby $pF[t] = mF[t] = \mathfrak{m}$. That is $pF[t]$ is a maximal ideal.
Generally $t - a$ is irreducible, for any $a \in F$, because of $\deg(t - a) = 1$. Thus by the above $(t - a)F[t]$ is a maximal ideal of $F[t]$. Conversely a maximal ideal $\mathfrak{m} \trianglelefteq_{\mathrm{i}} F[t]$ is of the form $pF[t]$ for some irreducible p. But if F is algebraically closed, then by (8.55.(f)) $\deg(p) = 1$. That is $p = ut - v$ for some $u, v \in F$ with $u \neq 0$. By taking $a := u^{-1}v$ we get $(t - a)F[t] = u(t - a)F[t] = (ut - v)F[t] = \mathfrak{m}$. And hence we also have the identity of the maximal spectrum of $F[t]$. □

Proof of (8.57):

(i) As $R[t \mid A]$ is a free R-module, having the basis $\{\, t^\alpha \mid \alpha \in A \,\}$ we have $\dim(R[t \mid A]) = |A|$ and thereby we have proved the claim in remark (3.67) already.

(ii) By definition $R[t_i \mid i \in I]$ is just the polynomial ring $R[t \mid A]$ for the commutative monoid $A = \mathbb{N}^{\oplus I}$. So let us take a closer look at the cardinality of A: If I is finite, say $\#I = n$, then $A = \mathbb{N}^n$ and thereby $|A| = |\mathbb{N}|$, because of (0.38.(iv).(c)) or alternatively, by (0.35.(ii)). If I is infinite, then never

the less any $\alpha \in A$ only has finitely many non-zero entries, that is $A = \mathcal{F}_0(I, \mathbb{N})$ in the notation of (3.67). And thereby A can be mapped injectively into the set $\Omega(I \times \mathbb{N})$ of finite subsets of $I \times \mathbb{N}$

$$A \hookrightarrow \Omega(I \times \mathbb{N}) : \alpha \mapsto \{ (i, \alpha_i) \mid i \in I, \alpha_i \neq 0 \}$$

Then we can use items (v).(d) and (v).(b) of proposition (0.38) again, this time, as I is infinite, we get $|A| \leq |\Omega(I \times \mathbb{N})| = |I \times \mathbb{N}|$. If I is infinite we also have $|\mathbb{N}| \leq |I|$, such that in any case

$$|A| \leq \max\{ |\mathbb{N}|, |I| \}$$

Conversely $I \hookrightarrow A : i \mapsto \delta_i$ clearly is injective, such that $|I| \leq |A|$. And if we fix any $i \in I$ then $\mathbb{N} \hookrightarrow A : n \mapsto n\delta_i$ is another injective map, that also guarantees $|\mathbb{N}| \leq |A|$. Altogether we get $|A| = \max\{ |\mathbb{N}|, |I| \}$ and the rest is (i): From this we know $|R[t_i \mid i \in I]| = \max\{ |A|, |R| \}$ and as we have just seen $|A| = \max\{ |\mathbb{N}|, |I| \}$ this turns into the claim $|R[t_i \mid i \in I]| = \max\{ |\mathbb{N}|, |I|, |R| \}$.

(iii) For any polynomial $f \in R[t]$ let $V_f := \{ x \in S \mid f(x) = 0 \} \subseteq S$. As $S : R$ is algebraic any $s \in S$ is contained in some V_f, that is we have

$$S = \bigcup_{f \in R[t]} V_f$$

And as S is an integral domain any V_f is finite. Also $R[t]$ is infinite, as we have an injection $\mathbb{N} \hookrightarrow R[t] : n \mapsto t^n$. But then we can use (0.38.(vii)) to see, that the cardinality of the union cannot exceed the cardinality of $R[t]$. And by (ii) we know

$$|S| = |\bigcup_{f \in R[t]} V_f| \leq |R[t]| = \max\{ |\mathbb{N}|, |R| \}$$

(iv) The prime field of E either is $P = \mathbb{Z}_p$ for $p = \text{CHAR}(E) \neq 0$ or $P = \mathbb{Q}$ in case $\text{CHAR}(E) = 0$, according to (2.107.(iv)). Thus in both cases P is countable, that is $|P| \leq |\mathbb{N}|$. Now choose a transcendence basis $U \subseteq F$ of $F : P$, that is (1) $F : P[U]$ is algebraic and (2) U is algebraically independent. Because of (2) we get an isomorphism of the following form from (8.46.(i))

$$P[t_u \mid u \in U] \xrightarrow{\sim} P[U] : t_u \mapsto u$$

In particular we get $|P[U]| = |P[t_u \mid u \in U]| = \max\{ |\mathbb{N}|, |P|, |U| \}$, where the latter identity is (ii). But we have already seen $|P| \leq |\mathbb{N}|$ so we can omit $|P|$ in this maximum and $|U|$ is the transcendence degree of $F : U$ by definition. Thus we are left with

$$|P[U]| = \max\{ |\mathbb{N}|, \text{trdeg}(F : P) \}$$

Yet a transcendence basis also satisfies (1) above, that is $F : P[U]$ is algebraic. And in (iii) we have seen that in this case $|F| = |P[U]|$. Combining this with the identity above we arrive at the claim $|F| = \max\{ |\mathbb{N}|, \text{trdeg}(F : P) \}$.

(v) If I is finite, then $R[t_i \mid i \in I]$ is finitely generated and as R is a notherian ring, the Hilbert Basis theorem (2.42) makes $R[t_i \mid i \in I]$ a noetherian ring again and thereby $\mathfrak{a}$ is finitely

generated. That is statement (1) of the claim. For statement (2) the set I is infinite. Let $\Omega(I) := \{\, \omega \subseteq I \mid \#\omega < \infty \,\}$ be the set of finite subsets of I. Then for any $\omega \in \Omega(I)$ the ring

$$R_\omega \;:=\; R[t_i \mid i \in \omega]$$

can be seen as a subring of $R[t_i \mid i \in I]$. By construction R_ω is finitely generated and hence by (1) $\mathfrak{a}_\omega := \mathfrak{a} \cap R_\omega$ is finitely generated. Let $A_\omega \subseteq R_\omega \subseteq R[t_i \mid i \in I]$ be a finite set, such that $\mathfrak{a}_\omega = \langle A_\omega \rangle_{\mathfrak{i}}$ and take

$$A \;:=\; \bigcup_{\omega \in \Omega(I)} A_\omega$$

By (7.23.(i)) any $f \in R[t_i \mid i \in I]$ is contained in some $f \in R_\omega$, for a sufficient $\omega \in \Omega(I)$. In particular any $f \in \mathfrak{a}$ is contained in some $f \in \mathfrak{a}_\omega = \mathfrak{a} \cap R_\omega$ for the same $\omega \in \Omega(I)$. And thereby

$$\mathfrak{a} \;=\; \bigcup_{\omega \in \Omega(I)} \mathfrak{a}_\omega \;\subseteq\; \sum_{\omega \in \Omega(I)} \mathfrak{a}_\omega \;\subseteq\; \mathfrak{a}$$

Generally the union generates the sum, but as the union is an ideal already, that contains any $\mathfrak{a}_\omega$, it also contains their sum and thereby the union and sum are identical. Now, as any $\mathfrak{a}_\omega$ is generated by A_ω, the union A of these sets generates all the ideals $\mathfrak{a}_\omega$ and thereby it generates $\mathfrak{a}$:

$$\langle A \rangle_{\mathfrak{i}} \;=\; \sum_{\omega \in \Omega(I)} \langle A_\omega \rangle_{\mathfrak{i}} \;=\; \sum_{\omega \in \Omega(I)} \mathfrak{a}_\omega \;=\; \mathfrak{a}$$

As I is infinite we have $|\Omega(I)| = |I|$, according to property (d) of (0.38.(v)). And as any A_ω is finite (0.38.(vii)) tells us, that the cardinality of A is bounded by the cardinality of the index set

$$|A| \;\leq\; |\Omega(I)| \;=\; |I|$$

□

Proof of (8.66):

- Let us first prove the implication (a) $\implies$ (b) for saturated CPI of R: Suppose $\mathcal{P} = (\mathfrak{p}_0, \ldots, \mathfrak{p}_m)$ is a maximal element of $\mathrm{CPI}^{\mathfrak{q}}_{\mathfrak{p}}(R)$ and consider some prime ideal $\mathfrak{p}$ such that $\mathfrak{p}_{k-1} \subseteq \mathfrak{p} \subseteq \mathfrak{p}_k$. If we had $\mathfrak{p}_{k-1} \neq \mathfrak{p}$ and $\mathfrak{p}_k \neq \mathfrak{p}$, then we could extend $\mathcal{P}$ to $\mathcal{P}' := (\mathfrak{p}_0, \ldots, \mathfrak{p}_{k-1}, \mathfrak{p}, \mathfrak{p}_k, \ldots, \mathfrak{p}_m)$. But then $\mathcal{P} < \mathcal{P}'$ would contradict the maximality of $\mathcal{P}$.

 Conversely suppose $(\mathfrak{p}_0, \ldots, \mathfrak{p}_m) \leq (\mathfrak{q}_0, \ldots, \mathfrak{q}_n)$ for some CPI with $\mathfrak{q}_0 = \mathfrak{p}_0$ and $\mathfrak{q}_n = \mathfrak{p}_m$. If we had $m < n$, then we could take $k \in 1 \ldots n-1$ be the minimal number, such that $\mathfrak{p} := \mathfrak{q}_k$ does not belong to $\{\, \mathfrak{p}_0, \ldots, \mathfrak{p}_m \,\}$. As k is minimal, we still have $\mathfrak{p}_{k-1} = \mathfrak{p}_{k-1} \subset \mathfrak{p}$. By assumption $(\mathfrak{p}_0, \ldots, \mathfrak{p}_m) \leq (\mathfrak{q}_0, \ldots, \mathfrak{q}_n)$ there is some $l \in k+1 \ldots n$ with $\mathfrak{p}_k = \mathfrak{q}_l$. And as $\mathfrak{p} = \mathfrak{q}_k \subset \mathfrak{q}_l = \mathfrak{p}_k$ we also have $\mathfrak{p} \subset \mathfrak{p}_k$. This contradicts (b), such that we have $m = n$ and thereby $(\mathfrak{p}_0, \ldots, \mathfrak{p}_m) = (\mathfrak{q}_0, \ldots, \mathfrak{q}_n)$.

- Let us now prove the implication (a) $\implies$ (b) for maximal CPI of R, that is $\mathcal{P} = (\mathfrak{p}_0, \ldots, \mathfrak{p}_m)$ is a maximal element of $\mathrm{CPI}(R)$ and we have to prove the properties (1) to (3) of (b). If $\mathcal{P}$ was not saturated, then there was some CPI $\mathcal{P}'$ with $\mathcal{P} < \mathcal{P}'$ which is ruled out by (a). If $\mathfrak{p}_m$ wasn't maximal, then by (2.4.(ii)) there was some maximal ideal $\mathfrak{m} \trianglelefteq_{\mathfrak{i}} R$ with $\mathfrak{p}_m \subseteq \mathfrak{p}$. But as $\mathfrak{p}_m$ isn't

maximal itself we have $\mathfrak{p}_m \neq \mathfrak{m}$. Also any maximal ideal is prime and hence $\mathcal{P}' := (\mathfrak{p}_0, \ldots, \mathfrak{p}_m, \mathfrak{m})$ would be a CPI of R, extending $\mathcal{P}$, contradicting the maximality of $\mathcal{P}$ again. Analogously, if $\mathfrak{p}_0$ wasn't minimal, then there was a prime ideal $\mathfrak{p} \subset \mathfrak{p}_0$ such that $\mathcal{P}' := (\mathfrak{p}, \mathfrak{p}_0, \ldots, \mathfrak{p}_m)$ would be a CPI of R, extending $\mathcal{P}$. Thus (1) to (3) have to be satisfied.

Conversely suppose $\mathcal{P} = (\mathfrak{p}_0, \ldots, \mathfrak{p}_m)$ satisfies (1) to (3) of (b) and consider any $\mathcal{P}' = (\mathfrak{q}_0, \ldots, \mathfrak{q}_n)$ with $\mathcal{P} \leq \mathcal{P}'$. In particular there is some $i \in 0 \ldots n$ such that $\mathfrak{p}_0 = \mathfrak{q}_i$. Suppose we had $i > 0$, then $\mathfrak{q}_0 \subset \mathfrak{q}_i = \mathfrak{p}_0$ such that $\mathfrak{p}_0$ would not be minimal. Therefore we have $i = 0$ and that is $\mathfrak{q}_0 = \mathfrak{p}_0$. Likewise there is some $j \in 0 \ldots n$ with $\mathfrak{p}_m = \mathfrak{q}_j$. Suppose we had $j < n$, then $\mathfrak{p}_m = \mathfrak{q}_j \subset \mathfrak{q}_n \neq R$ which contradicts the maximality of $\mathfrak{p}_m$. Therefore we also have $\mathfrak{p}_m = \mathfrak{q}_n$. That is $\mathcal{P}'$ satisfies the properties required in (a) for the saturated chain $\mathcal{P}$ and therefore we can conclude $\mathcal{P} = \mathcal{P}'$ which is the maximality of $\mathcal{P}$ in $\mathrm{CPI}(R)$.

□

Proof of (8.75):

(i) Let R be holodimensional and $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ be a prime ideal, then we will prove the identity for the Krull-dimension of R in (i) first: As $\mathrm{kdim}(R) < \infty$ we can find a maximal CPI $\mathcal{P} = (\mathfrak{p}_0, \ldots, \mathfrak{p}_n)$ that extends $(\mathfrak{p}) \in \mathrm{CPI}(R)$. From $(\mathfrak{p}) \leq \mathcal{P}$ we find some $k \in 0 \ldots n$ such that $\mathfrak{p}_k = \mathfrak{p}$. But then we conclude:

As $(\mathfrak{p}_0, \ldots, \mathfrak{p}_k)$ is a CPI with $\mathfrak{p}_k = \mathfrak{p}$ we have $\mathrm{height}(\mathfrak{p}) \geq k$. And as $(\mathfrak{p}_k/\mathfrak{p}, \ldots, \mathfrak{p}_n/\mathfrak{p})$ is a CPI in $R/\mathfrak{p}$ we also have $\mathrm{kdim}(R/\mathfrak{p}) \geq n - k$. Together this is

$$\mathrm{kdim}(R) \;=\; n \;=\; (n-k)+k \;\leq\; \mathrm{kdim}\left(R \Big/ \mathfrak{p}\right) + \mathrm{height}(\mathfrak{p}) \;\leq\; \mathrm{kdim}(R)$$

where the latter estimate is (8.69.(x)). Together this implies the equality of the Krull-dimension of R and the Krull-dimension of $R/\mathfrak{p}$ plus the height of $\mathfrak{p}$.

- Let R be a holodimensional ring, then we will now prove that R also is equidimensional: Consider any maximal ideal $\mathfrak{m}$ of R, as R has finite Krull-dimension we have $\mathrm{height}(\mathfrak{m}) \leq \mathrm{kdim}(R) < \infty$. Hence we may pick up a CPI $\mathcal{P} = (\mathfrak{p}_0, \ldots, \mathfrak{p}_m)$ of R such that $\mathfrak{p}_m = \mathfrak{m}$ and $m = \mathrm{height}(\mathfrak{m})$. This CPI is maximal - if it could be extended, then the extended chain would be longer. And as $\mathfrak{p}_m = \mathfrak{m}$ is maximal this would increase the height of $\mathfrak{m}$, which is fixed at m.

 Yet as R is holodimensional, this means $\mathrm{height}(\mathfrak{m}) = \ell(\mathcal{P}) = \mathrm{kdim}(R)$. And as this is true for any maximal ideal $\mathfrak{m}$ of R, all maximal ideals of R share the same height, namely $\mathrm{kdim}(R)$.

- Let R be a holodimensional ring, then we will now prove that R also is catenary: Consider any two prime ideals $\mathfrak{p}$, $\mathfrak{q}$ of R such that $\mathfrak{p} \subset \mathfrak{q}$. As $\mathrm{kdim}(R) < \infty$ we can find a maximal CPI $\mathcal{P}$ in R such that $(\mathfrak{p}, \mathfrak{q}) \leq \mathcal{P}$. Say $\mathcal{P} = (\mathfrak{p}_0, \ldots, \mathfrak{p}_n)$ then there are some $0 \leq i < j \leq n$ such that $\mathfrak{p}_i = \mathfrak{p}$ and $\mathfrak{p}_j = \mathfrak{q}$. As $\mathcal{P}$ is maximal, the subchain $\mathcal{P}_0 := (\mathfrak{p}_i, \ldots, \mathfrak{p}_j) \leq \mathcal{P}$ is saturated. In particular property (1) of catenary rings is satisfied.

 And as R is holodimensional we also have $n = \ell(\mathcal{P}) = \mathrm{kdim}(R)$. For property (2) of catenary rings, we have to look at any other saturated CPI $\mathcal{Q} = (\mathfrak{q}_0, \ldots, \mathfrak{q}_m) \in \mathrm{CPI}^{\mathfrak{q}}_{\mathfrak{p}}(R)$. Then by construction

$$(\mathfrak{p}_0, \ldots, \mathfrak{p}_{i-1}, \mathfrak{q}_0, \ldots, \mathfrak{q}_m, \mathfrak{p}_{j+1}, \ldots, \mathfrak{p}_n)$$

also is a maximal CPI of R: As $\mathfrak{p}_i = \mathfrak{p} = \mathfrak{q}_0$ and $\mathfrak{p}_j = \mathfrak{p} = \mathfrak{q}_m$ the CPI $\mathcal{Q}$ can be inserted seamlessly. Still $\mathfrak{p}_0$ is a minimal prime and $\mathfrak{p}_n$ is a maximal ideal and we cannot insert any prime ideal in between, as all the chains $(\mathfrak{p}_0, \ldots, \mathfrak{p}_{i-1})$, $\mathcal{Q}$ and $(\mathfrak{p}_{j+1}, \ldots, \mathfrak{p}_n)$ are saturated. But as this CPI is maximal it is of length $\operatorname{kdim}(R)$ as well. And this implies $\ell(\mathcal{Q}) = \ell(\mathcal{P})$. As we have fixed $\mathcal{P}$ and this is true for any saturated $\mathcal{Q} \in \operatorname{CPI}_{\mathfrak{p}}^{\mathfrak{q}}(R)$, all these CPI must be of the same length.

(iii) Let us now prove (iii): First of all $\operatorname{kdim}(R/\mathfrak{p}) \leq \operatorname{kdim}(R) < \infty$ such that $R/\mathfrak{p}$ has finite Krull-dimension again. So consider any maximal CPI $\mathcal{U} = (\mathfrak{u}_0, \ldots, \mathfrak{u}_m)$ of $R/\mathfrak{p}$. As this is maximal $\mathfrak{u}_0$ is a minimal prime of $R/\mathfrak{p}$, but as $\mathfrak{p}$ is a prime ideal $R/\mathfrak{p}$ is an integral domain, so the one and only minimal prime of $R/\mathfrak{p}$ is the zero ideal $\mathfrak{u}_0 = 0$.

By the correspondence theorem of ideals, any $\mathfrak{u}_i$ is of the form $\mathfrak{u}_i = \mathfrak{q}_i/\mathfrak{p}$ for some $\mathfrak{q}_i \in \operatorname{Spec}(R)$ with $\mathfrak{p} \subseteq \mathfrak{q}_i$. That is we find a CPI $\mathcal{Q} = (\mathfrak{q}_0, \ldots, \mathfrak{q}_m)$ of R. And as $\mathfrak{q}_0/\mathfrak{p} = \mathfrak{u}_0 = 0$ we have $\mathfrak{q}_0 = \mathfrak{p}$. Now pick up a CPI $\mathcal{P} = (\mathfrak{p}_0, \ldots, \mathfrak{p}_k)$ of R such that $\mathfrak{p}_k = \mathfrak{p}$ and $k = \operatorname{height}(\mathfrak{p})$. As we have $\mathfrak{p}_k = \mathfrak{p} = \mathfrak{q}_0$ we can concatenate these CPI to a single chain

$$\mathcal{M} := (\mathfrak{p}_0, \ldots, \mathfrak{p}_k = \mathfrak{q}_0, \mathfrak{q}_1, \ldots, \mathfrak{q}_m)$$

Both $\mathcal{P}$ and $\mathcal{U}$ are maximal and hence saturated. This means $\mathcal{Q}$ is saturated again (by the correspondence of ideals). Also $\mathfrak{q}_m$ is a maximal ideal, as $\mathfrak{u}_m$ is, too. Altogether $\mathcal{M}$ is a maximal CPI of R and thereby, as R is holodimensional

$$\operatorname{kdim}(R) \;=\; \ell(\mathcal{M}) \;=\; k+m \;=\; \operatorname{height}(\mathfrak{p}) + \ell(\mathcal{U})$$

Therefore $\ell(\mathcal{U}) = \operatorname{kdim}(R) - \operatorname{height}(\mathfrak{p})$ is independent of the specific ideals that build up the maximal chain $\mathcal{U}$. As there is some CPI $\mathcal{V} \in \operatorname{CPI}(R/\mathfrak{p})$ with $\ell(\mathcal{V}) = \operatorname{kdim}(R/\mathfrak{p})$ and any such CPI is maximal we conclude $\ell(\mathcal{U}) = \ell(\mathcal{V}) = \operatorname{kdim}(R/\mathfrak{p})$ for any maximal CPI $\mathcal{U}$ of $R/\mathfrak{p}$. And this means $R/\mathfrak{p}$ is holodimensional, too.

(iv) We start with (a) $\Longrightarrow$ (b): As $\mathfrak{q} \trianglelefteq_{\mathrm{i}} R$ is of finite height, so is $\mathfrak{q}/\mathfrak{p} \trianglelefteq_{\mathrm{i}} R/\mathfrak{p}$, by the correspondence theorem of ideals (8.65.(i)). So let us take any CPI $\mathfrak{q}_0/\mathfrak{p} \subset \ldots \subset \mathfrak{q}_s/\mathfrak{p}$ with $\mathfrak{q}_s/\mathfrak{p} = \mathfrak{q}/\mathfrak{p}$ and $s = \operatorname{height}(\mathfrak{q}/\mathfrak{p})$. Note that this is $\mathfrak{q}_s = \mathfrak{q}$. Also $\mathfrak{p}_0/\mathfrak{p} = 0$: As $R/\mathfrak{p}$ is an integral domain 0 is a prime ideal and hence we could append $0 \subset \mathfrak{q}_0/\mathfrak{p} \subset \ldots \subset \mathfrak{q}_s/\mathfrak{p}$, which would be a CPI of length $s+1$, exceeding s. And this means $\mathfrak{q}_0 = \mathfrak{p}$, as well. Now suppose there was some $\mathfrak{q}' \in \operatorname{Spec}(R)$ such that $\mathfrak{q}_{k-1} \subset \mathfrak{q}' \subset \mathfrak{q}_k$ then we also had $\mathfrak{q}_{k-1}/\mathfrak{p} \subset \mathfrak{q}'/\mathfrak{p} \subset \mathfrak{q}_k/\mathfrak{p}$ such that we could find a CPI of length $s+1$ ending in $\mathfrak{q}/\mathfrak{p}$. As s is maximal with this property this means $\mathfrak{q}_{k-1} \subset_* \mathfrak{q}_k$ such that by assumption (a) we have $\operatorname{height}(\mathfrak{q}_k) = \operatorname{height}(\mathfrak{q}_{k-1}) + 1$. And from this we get

$$\operatorname{height}(\mathfrak{q}) - \operatorname{height}(\mathfrak{p}) \;=\; \sum_{k=1}^{s} \big(\operatorname{height}(\mathfrak{q}_k) - \operatorname{height}(\mathfrak{q}_{k-1})\big) \;=\; s \;=\; \operatorname{height}\left(\mathfrak{q} \Big/ \mathfrak{p}\right)$$

Conversely for (b) $\Longrightarrow$ (a): If $\mathfrak{p} \subset_* \mathfrak{q}$ then $(\mathfrak{p}, \mathfrak{q})$ is a CPI in R. Consider any CPI in $R/\mathfrak{p}$ such that $0 = \mathfrak{p}_0/\mathfrak{p} \subset \ldots \subset \mathfrak{p}_r/\mathfrak{p}$ such that $\mathfrak{p}_0 = \mathfrak{p}$ and $\mathfrak{p}_r = \mathfrak{q}$. Then we have $\mathfrak{p} = \mathfrak{p}_0 \subset \mathfrak{p}_1 \subseteq \mathfrak{p}_r = \mathfrak{q}$, by the correspondence theorem of ideals. But as $\mathfrak{q}$ is minimal over $\mathfrak{p}$ and $\mathfrak{p} \subset \mathfrak{p}_1$ this is $\mathfrak{p}_1 = \mathfrak{q}$, in other words $r = 1$. Therefore we have $\operatorname{height}(\mathfrak{q}/\mathfrak{p}) = 1$ and due to (b) this yields $\operatorname{height}(\mathfrak{q}) - \operatorname{height}(\mathfrak{p}) = 1$. But this already is (a).

It remains to prove that (a) and (b) imply R to be catenary. So fix any two nested primes $\mathfrak{p} \subseteq \mathfrak{q}$ of R. As $n := \text{height}(\mathfrak{q}) < \infty$ is finite the following set is bounded by n from above

$$\left\{ s \in \mathbb{N} \;\middle|\; (\mathfrak{q}_0, \ldots, \mathfrak{q}_s) \in \text{CPI}_{\mathfrak{p}}^{\mathfrak{q}} \right\}$$

In particular we can fix any CPI $\mathfrak{p} = \mathfrak{q}_0 \subset \ldots \subset \mathfrak{q}_s = \mathfrak{q}$ of maximal length s. And by the maximality of s, this CPI is saturated - if we could insert some $\mathfrak{p}' \in \text{Spec}(R)$ in between any $\mathfrak{q}_{k-1} \subset \mathfrak{q}_k$ we would get a CPI longer than s. Thus $\mathfrak{p}$ and $\mathfrak{q}$ can be connected by a saturated CPI.

Now consider any saturated CPI $\mathfrak{p} = \mathfrak{p}_0 \subset \ldots \subset \mathfrak{p}_r = \mathfrak{q}$. Being saturated means $\mathfrak{p}_{k-1} \subset_* \mathfrak{p}_k$ for any $k \in 1 \ldots r$. But by (a) this means $\text{height}(\mathfrak{p}_k) = \text{height}(\mathfrak{p}_{k-1}) + 1$. But as in (a) $\implies$ (b) before we hence get

$$r \;=\; \sum_{k=1}^{r} \big(\text{height}(\mathfrak{p}_k) - \text{height}(\mathfrak{p}_{k-1}) \big) \;=\; \text{height}(\mathfrak{q}) - \text{height}(\mathfrak{p})$$

That is the length of all saturated CPIs from $\mathfrak{p}$ to $\mathfrak{q}$ is fixed to be $\text{height}(\mathfrak{q}) - \text{height}(\mathfrak{p})$, which is invariant under the respective CPI chosen. And thereby R is catenary.

(v) The proof of (v) follows the same lines as the proof of (iii): First of all by (8.69.(ix)) we have $\text{kdim}(R_{\mathfrak{p}}) = \text{height}(\mathfrak{p}) \leq \text{kdim}(R) < \infty$ again. So consider any maximal CPI $\mathcal{U} = (\mathfrak{u}_0, \ldots, \mathfrak{u}_m)$ of $R_{\mathfrak{p}}$. As this is maximal $\mathfrak{u}_m$ is a maximal ideal, so we have $\mathfrak{u}_m = \mathfrak{p}R_{\mathfrak{p}}$, as this is the only maximal ideal available in $R_{\mathfrak{p}}$.

Now, by the correspondence theorem of ideals in localisations, any $\mathfrak{u}_i$ is if the form $\mathfrak{u}_i = \mathfrak{p}_i R_{\mathfrak{p}}$ for some prime ideal $\mathfrak{p}_i \trianglelefteq_{\mathfrak{i}} R$ with $\mathfrak{p}_i \subseteq \mathfrak{p} = \mathfrak{p}_m$, also refer to (8.65.(ii)) for this. Hence we have found a CPI $\mathcal{P} = (\mathfrak{p}_0, \ldots, \mathfrak{p}_m)$ of R of length m, with $\mathfrak{p}_m = \mathfrak{p}$.

Now pick up a CPI $\mathcal{V} = (\mathfrak{v}_0, \ldots, \mathfrak{v}_n)$ of $R/\mathfrak{p}$ such that $n = \text{kdim}(R/\mathfrak{p})$. As in the proof of (ii) above any $\mathfrak{v}_j$ is of the form $\mathfrak{v}_j = \mathfrak{q}_j/\mathfrak{p}$ for some prime ideal $\mathfrak{q}_j \trianglelefteq_{\mathfrak{i}} R$ and $\mathfrak{p}_0 = \mathfrak{p}$ as $\mathfrak{v}_0 = 0$. And as before $\mathcal{Q} = (\mathfrak{q}_0, \ldots, \mathfrak{q}_n)$ is a CPI of R of length n. As we have $\mathfrak{p}_m = \mathfrak{p} = \mathfrak{q}_0$ we can concatenate these CPI to a single chain, once again

$$\mathcal{M} \;:=\; (\mathfrak{p}_0, \ldots, \mathfrak{p}_m = \mathfrak{q}_0, \mathfrak{q}_1, \ldots, \mathfrak{q}_n)$$

Both $\mathcal{U}$ and $\mathcal{V}$ are maximal and hence saturated. This means both $\mathcal{P}$ and $\mathcal{Q}$ are saturated again (by the correspondence of ideals). Also $\mathfrak{q}_n$ is a maximal ideal, as $\mathfrak{v}_n$ is, too. And $\mathfrak{p}_0$ is a minimal prime, as $\mathcal{U}$ is maximal and hence $\mathfrak{u}_0$ is a minimal prime, too. Altogether $\mathcal{M}$ is a maximal CPI of R and thereby, as R is holodimensional

$$\text{kdim}(R) \;=\; \ell(\mathcal{M}) \;=\; m + n \;=\; \ell(\mathcal{U}) + \text{kdim}\left(R \Big/ \mathfrak{p} \right)$$

Therefore $\ell(\mathcal{U}) = \text{kdim}(R) - \text{kdim}(R/\mathfrak{p})$ is independent of the specific ideals that build up the maximal chain $\mathcal{U}$. As there is some CPI $\mathcal{V} \in \text{CPI}(R_{\mathfrak{p}})$ with $\ell(\mathcal{V}) = \text{kdim}(R_{\mathfrak{p}})$ and any such CPI is maximal we conclude $\ell(\mathcal{U}) = \ell(\mathcal{V}) = \text{kdim}(R_{\mathfrak{p}})$ for any maximal CPI $\mathcal{U}$ of $R_{\mathfrak{p}}$. And this means $R_{\mathfrak{p}}$ is holodimensional, too.

(ii) We are now ready to prove (ii): Consider a saturated CPI $\mathfrak{p}_0 \subset \ldots \subset \mathfrak{p}_r$ such that $\mathfrak{p}_0 = \mathfrak{p}$ and

$\mathfrak{p}_r = \mathfrak{q}$. By the correspondence theorem (8.65.(i)) we get a saturated CPI in $R/\mathfrak{p}$ by going to quotients $0 = \mathfrak{p}_0/\mathfrak{p} \subset \ldots \subset \mathfrak{p}_r/\mathfrak{p}$. As $R/\mathfrak{p}$ is holodimensional (in particular $\operatorname{kdim}(R/\mathfrak{p}) < \infty$) by assumption, we can append this to a maximal CPI of $R/\mathfrak{p}$

$$0 \;=\; \mathfrak{p}_0\Big/_{\mathfrak{p}} \;\subset\; \mathfrak{p}_0\Big/_{\mathfrak{p}} \;\subset\; \mathfrak{p}_s\Big/_{\mathfrak{p}}$$

where $s = \operatorname{kdim}(R/\mathfrak{p})$. As this chain is maximal $\mathfrak{p}_s \trianglelefteq_{\mathrm{i}} R$ is a maximal ideal. For any $k \in r \ldots s$ we have $\mathfrak{q} = \mathfrak{p}_r \subseteq \mathfrak{p}_k$ such that by (8.65.(i)) we obtain another CPI, in $R/\mathfrak{q}$ this time

$$0 \;=\; \mathfrak{p}_r\Big/_{\mathfrak{q}} \;\subset\; \ldots \;\subset\; \mathfrak{p}_s\Big/_{\mathfrak{q}}$$

This CPI is saturated, by correspondence, and as $\mathfrak{p}_s/\mathfrak{q}$ is a maximal ideal of $R/\mathfrak{q}$ and $\mathfrak{p}_r/\mathfrak{q} = 0$ this chain is maximal, too. As $R/\mathfrak{q}$ is holodimensional, this again means $\operatorname{kdim}(R/\mathfrak{q}) = s - r$, as this is the length of this chain. Thus we can express the length r of the chain in the beginning in terms

$$\operatorname{kdim}\left(R\Big/_{\mathfrak{p}}\right) - \operatorname{kdim}\left(R\Big/_{\mathfrak{q}}\right) \;=\; s - (s-r) \;=\; r$$

And if we use the dimension formula of (i) for $R/\mathfrak{p}$ and $R/\mathfrak{q}$, which are both holodimensional, we can also express this in terms of the height of these ideals

$$\begin{aligned}\operatorname{height}(\mathfrak{q}) - \operatorname{height}(\mathfrak{p}) &= \operatorname{kdim}(R) - \operatorname{kdim}\left(R\Big/_{\mathfrak{q}}\right) - \operatorname{kdim}(R) + \operatorname{kdim}\left(R\Big/_{\mathfrak{p}}\right)\\ &= \operatorname{kdim}\left(R\Big/_{\mathfrak{p}}\right) - \operatorname{kdim}\left(R\Big/_{\mathfrak{p}}\right) \;=\; r\end{aligned}$$

- By the above we know, that $\ell(\mathcal{P}) = \operatorname{height}(\mathfrak{q}) - \operatorname{height}(\mathfrak{p})$ for any saturated CPI $\mathcal{P}$ ranging from $\mathfrak{p}$ to $\mathfrak{q}$. To prove the final equality $\operatorname{height}(\mathfrak{q}/\mathfrak{p}) = \operatorname{height}(\mathfrak{q}) - \operatorname{height}(\mathfrak{p})$ we start with a CPI in $R/\mathfrak{p}$ that is of the form

$$\mathfrak{p}_0\Big/_{\mathfrak{p}} \;\subset\; \ldots \;\subset\; \mathfrak{p}_r\Big/_{\mathfrak{p}} \;=\; \mathfrak{q}\Big/_{\mathfrak{p}}$$

where $r = \operatorname{height}(\mathfrak{q}/\mathfrak{p})$. As r is maximal and $R/\mathfrak{p}$ is an integral domain, we have $\mathfrak{p}_0/\mathfrak{p} = 0$, which is $\mathfrak{p}_0 = \mathfrak{p}$. Also $\mathcal{P} = (\mathfrak{p}_0, \ldots, \mathfrak{p}_r)$ is saturated: If we could insert some $\mathfrak{p}' \in \operatorname{Spec}(R)$ at any position $\mathfrak{p}_{i-1} \subset \mathfrak{p}' \subset \mathfrak{p}_i$ then $\mathfrak{p}_{i-1}/\mathfrak{p} \subset \mathfrak{p}'/\mathfrak{p} \subset \mathfrak{p}_i/\mathfrak{p}$ which would yield a longer chain, that does not exist. Now, as $\mathcal{P}$ is a saturated chain ranging from $\mathfrak{p}$ to $\mathfrak{q}$, we get

$$\operatorname{height}(\mathfrak{q}) - \operatorname{height}(\mathfrak{p}) \;=\; \ell(\mathcal{P}) \;=\; r \;=\; \operatorname{height}\left(\mathfrak{q}\Big/_{\mathfrak{p}}\right)$$

(vi) As R is equidimensional, we have $\operatorname{kdim}(R) < \infty$ and hence we can choose some CPI $\mathcal{Q} = (\mathfrak{q}_0, \ldots, \mathfrak{q}_n)$ of R with $n = \operatorname{kdim}(R)$. Thereby $\mathcal{Q}$ is maximal and hence $\mathfrak{n} := \mathfrak{q}_n$ is a maximal ideal. In particular $\operatorname{height}(\mathfrak{n}) = n$, as

$$n \;\leq\; \operatorname{height}(\mathfrak{n}) \;\leq\; \operatorname{kdim}(R) \;=\; n$$

Now consider any maximal CPI $\mathcal{P} = (\mathfrak{p}_0, \ldots, \mathfrak{p}_m)$ of R. We have to show $\ell(\mathcal{P}) = \operatorname{kdim}(R)$, that is $m = n$. As $\mathcal{P}$ is maximal $\mathfrak{p}_0$ is a minimal prime and $\mathfrak{m} := \mathfrak{p}_m$ is a maximal ideal. Also $\mathcal{P}$ is saturated. Yet R is an integral domain, so the only minimal prime ideal available is $\mathfrak{p}_0 = 0$.

Now pick up a CPI $\mathcal{H} = (\mathfrak{h}_0, \ldots, \mathfrak{h}_r)$ of R such that $\mathfrak{h}_r = \mathfrak{m}$ and $r = \operatorname{height}(\mathfrak{m})$. Again, as $\mathcal{H}$ is a

chain that builds up the height of $\mathfrak{m}$ it must be saturated and $\mathfrak{h}_0 = 0$, as R is an integral domain. That is we have found two CPI $\mathcal{H}$ and $\mathcal{P} \in \mathrm{CPI}_0^{\mathfrak{m}}(R)$ that both are saturated and hence we have $r = \ell(\mathcal{H}) = \ell(\mathcal{P}) = m$ by property (2) of catenary rings. Yet $\mathfrak{m}$ is a maximal ideal and R also is equidimensional, such that $r = \mathrm{height}(\mathfrak{m}) = \mathrm{height}(\mathfrak{n}) = n$. Altogether we have found

$$\ell(\mathcal{P}) \;=\; m \;=\; r \;=\; n \;=\; \mathrm{kdim}(R)$$

□

Proof of (8.76):

(i) Let $\mathfrak{q}_0 \subset \mathfrak{q}_1 \subset \ldots \subset \mathfrak{q}_r$ be a maximal CPI in A. By the Noetherian normalisation theorem (8.52) there are some $z_1, \ldots, z_n \in A$ and $0 \leq k(0) \leq k(1) \leq \cdots \leq k(r) \leq n$ such that $\{ z_1, \ldots, z_n \}$ is algebraically independent, $A : P$ is finite and for any $i \in 0 \ldots r$ we get

$$\mathfrak{q}_i \cap P \;=\; z_1 P + \cdots + z_{k(i)} P$$

where $P = E[z_1, \ldots, z_n] \subseteq A$ and $n = \mathrm{trdeg}(A : E)$. As the chain is maximal and A is an integral domain, we have $\mathfrak{q}_0 = 0$ and hence $k(0) = 0$. Also, as the $\mathfrak{q}_i$ form a CPI and $A : P$ is integral (even finite) so do the restricted ideals $\mathfrak{p}_i := \mathfrak{q}_i \cap P$, according to the lying-over theorem (8.32.(iii))

$$0 = \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_r$$

As $\mathfrak{p}_i = \mathfrak{q}_i \cap P = z_1 P + \cdots + z_{k(i)} P$ we see that $0 = k(0) < k(1) < \cdots < k(r)$ as well, as $k(i-1) = k(i)$ would imply $\mathfrak{p}_{i-1} = \mathfrak{p}_i$ and hence $\mathfrak{q}_{i-1} = \mathfrak{q}_i$. In particular we conclude $r \leq n$.

- Now fix any $i \in 1 \ldots r$ and let $k := k(i-1)$, $m := n - k$. We also abbreviate $Q_i := A/\mathfrak{q}_{i-1}$ and $u_j := z_{j+k} + \mathfrak{q}_{i-1} \in Q_i$ for any $j \in 1 \ldots m$. With these notations let us prove, that

$$E[u_1, \ldots, u_m] \;=\; \{ p + \mathfrak{q}_{i-1} \mid p \in P \}$$

For any $q \in E[u_1, \ldots, u_m]$ there is some polynomial $f \in E[t_1, \ldots, t_m]$ such that $q = f(u_1, \ldots, u_m) = f(z_{i+k}, \ldots, z_n) + \mathfrak{q}_{i-1}$. As $P = E[z_1, \ldots, z_n]$ it is clear, that $p := f(z_{i+k}, \ldots, z_n) \in P$ and thereby $q = p + \mathfrak{q}_{i-1}$ is contained in the right-hand set. Conversely we start with some $p \in P$, that is $p = f(z_1, \ldots, z_n)$ for some polynomial $f \in E[t_1, \ldots, t_n]$. Note that for any $j \in 1 \ldots k$ we have $z_j \in z_j P \subseteq \mathfrak{q}_{i-1} \cap P \subseteq \mathfrak{q}_{i-1}$. That is $z_j + \mathfrak{q}_{i-1} = 0 + \mathfrak{q}_{i-1}$. And for $j \in k+1 \ldots n$ we have $z_j + \mathfrak{q}_{i-1} = u_{j-k}$ by construction. Thus we find

$$p + \mathfrak{q}_{i-1} \;=\; f\big(z_1 + \mathfrak{q}_{i-1}, \ldots, z_n + \mathfrak{q}_{i-1}\big) \;=\; f(0, \ldots, 0, u_1, \ldots, u_m)$$

That is $p + \mathfrak{q}_{i-1} = f(0, \ldots, 0, u_1, \ldots, u_m) \in E[u_1, \ldots, u_m]$. This establishes the inclusion from right to left and thereby the equality of these sets.

- In the next step we prove, that $\{ u_1, \ldots, u_m \} \subseteq Q_i$ is algebraically independent. To do this consider any polynomial $f \in E[t_1, \ldots, t_m]$ such that

$$0 + \mathfrak{q}_{i-1} \;=\; f(u_1, \ldots, u_m) \;=\; f(z_{k+1}, \ldots, z_n) + \mathfrak{q}_{i-1}$$

That is $p := f(z_{k+1},\dots,z_n) \in \mathfrak{q}_{i-1}$. But as $p \in P$ is clear, as well, we find, that p is contained, in $p \in \mathfrak{q}_{i-1} \cap P = z_1P + \cdots + z_kP \subseteq E[z_1,\dots,z_k]$. From the construction of p it is also clear, that $p \in E[z_{k+1},\dots,z_n]$ and therefore

$$p \;\in\; E[z_1,\dots,z_k] \cap E[z_{k+1},\dots,z_n] \;=\; E$$

As the sets of variables are mutually exclusive [recall that $\{ z_1,\dots,z_n \}$ is algebraically independent] the only polynomials that are contained in both sets are constant $p \in E$. But we have $p \in \mathfrak{q}_{i-1}$ and $\mathfrak{q}_{i-1} \neq A$, as it was a prime ideal. This only leaves $p = 0$ and as $\{ z_{k+1},\dots,z_n \}$ is algebraically independent, this means $f = 0$. That is $\{ u_1,\dots,u_m \}$ is algebraically independent, too.

- Denote the canonical epimorphism by $\varrho : A \twoheadrightarrow Q_i : x \mapsto x + \mathfrak{q}_{i-1}$. Two steps before we have shown $\varrho(P) = E[u_1,\dots,u_m]$. But $A : P$ is integral (even finite), as we gained it by noetherian normalisation. Now, as ϱ is surjective, (8.28) tells us, that $Q_i : E[u_1,\dots,u_m]$ is integral, too.

- Let us abbreviate $P_i := E[u_1,\dots,u_m] \subseteq Q_i$. As the $\{ u_1,\dots,u_m \}$ are algebraically independent, P_i is isomorphic to a polynomial ring in m variables such that the ideals $\mathfrak{u}_j := u_1P_i + \cdots + u_jP_i$ are prime and form a CPI in P_i, too

$$0 \;\subset\; \mathfrak{u}_1 \;\subset\; \dots \;\subset\; \mathfrak{u}_m$$

By construction $\varrho : P \twoheadrightarrow P_i : p \mapsto p + \mathfrak{q}_{i-1}$ is an epimorphism of algebras, as $z_j \in P = E[z_1,\dots,z_n]$ is mapped to $\varrho(z_j) = 0$ for $j \in 1\dots k$ and $\varrho(z_j) = u_{j-k} \in E[u_1,\dots,u_m] = P_i$ for $j \in k+1\dots n$. That is the kernel of this ϱ is given to be $z_1P \dots z_kP = \mathfrak{q}_{i-1} \cap P$ and thereby

$$P \Big/ \mathfrak{q}_{i-1} \cap P \;\xrightarrow{\sim}\; P_i \;:\; z_j \mapsto u_{j-k}$$

Let us denote $l := k(i) - k = k(i) - k(i-1) \in 1\dots m$, then the ideal $\mathfrak{q}_i \cap P = z_1P + \cdots + z_{k(i)}P$ is mapped to $\mathfrak{u}_l = u_1P_i + \cdots + u_lP_i$ under ϱ. We now claim the identity

$$\mathfrak{q}_i \Big/ \mathfrak{q}_{i-1} \cap P_i \;=\; u_1P_i + \cdots + u_lP_i \;=\; \mathfrak{u}_l$$

Let us agree to denote this ideal by $\mathfrak{v}_l := \mathfrak{q}_i/\mathfrak{q}_{i-1}$. The inclusion from right to left is easy as we already know $\mathfrak{u}_l = \varrho(\mathfrak{q}_i \cap P) \subseteq \varrho(\mathfrak{q}_i) = \mathfrak{q}_i/\mathfrak{q}_{i-1} = \mathfrak{v}_l$. For the converse inclusion we consider any $v = q + \mathfrak{q}_{i-1} \in \mathfrak{v}_l \cap P_i$. That is $q \in \mathfrak{q}_i$ and $v \in E[u_1,\dots,u_m]$. That is $v = f(u_1,\dots,u_m)$ for some polynomial f in m variables. Let us write this out

$$v \;=\; f(u_1,\dots,u_m) \;=\; \sum_{\alpha\in\mathbb{N}^l} \sum_{\beta\in\mathbb{N}^{m-l}} f[\alpha,\beta]\,(u_1,\dots,u_l)^\alpha (u_{l+1},\dots,u_m)^\beta$$

and let us abbreviate $f_\alpha := \sum_\beta f[\alpha,\beta]\,(u_{l+1},\dots,u_m)^\beta$ that is $v = \sum_\alpha f_\alpha\,(u_1,\dots,u_l)^\alpha$. Then we split v up into a part $\alpha = 0$ and the rest $\alpha \neq 0$. That is we write v as

$$v \;=\; f_0 + \sum_{\alpha\neq 0} f_\alpha\,(u_1,\dots,u_l)^\alpha$$

If $\alpha \neq 0$ there is some $j \in 1\dots l$ with $\alpha_j \geq 1$ and therefore u^α contains u_j as a factor. Hence all the

$f_\alpha\,(u_1,\ldots,u_l)^\alpha$ are contained in $u_1P_i+\cdots+u_lP_i$ and we have already argued, that this in turn is contained in $\mathfrak{v}_l$. Thus we have $f_\alpha\,(u_1,\ldots,u_l)^\alpha\in\mathfrak{v}_l$ for any $\alpha\neq 0$ and therefore

$$\sum_{\beta\in\mathbb{N}^{m-l}} f[0,\beta]\,(u_{l+1},\ldots,u_m)^\beta \;=\; f_0 \;=\; v-\sum_{\alpha\neq 0} f_\alpha\,(u_1,\ldots,u_l)^\alpha \;\in\; \mathfrak{v}_l \;=\; \mathfrak{q}_i\Big/\mathfrak{q}_{i-1}$$

But as $f_0\in P_i$ there is a uniquely determined $g+\mathfrak{q}_{i-1}\cap P$ such that $\varrho(g)=f_0$, by the above isomorphism. This g obviously is

$$g \;:=\; \sum_{\beta\in\mathbb{N}^{m-l}} f[0,\beta]\,(z_{k(i)+1},\ldots,z_n)^\beta$$

If $g\neq 0$ then $g\notin z_1P+\cdots+z_{k(i)}P=\mathfrak{q}_i\cap P$ is clear. But as $g\in P$ is a given, we can conclude $g=0$ or $g\notin\mathfrak{q}_i$. But as $\mathfrak{q}_{i-1}\cap P\subseteq\mathfrak{q}_{i-1}$ we have $g+\mathfrak{q}_{i-1}=f_0\in\mathfrak{q}_i/\mathfrak{q}_{i-1}$ that is $g+\mathfrak{q}_{i-1}=q+\mathfrak{q}_{i-1}$ for some $q\in\mathfrak{q}_i$. As $\mathfrak{q}_{i-1}\subseteq\mathfrak{q}_i$ we could diffuse further and only regard $g+\mathfrak{q}_i=q+\mathfrak{q}_i=0+\mathfrak{q}_i$ such that $g\in\mathfrak{q}_i$ as well. This only leaves $g=0$ and hence $f_0=0$ such that

$$v \;=\; f(u_1,\ldots,u_m) \;=\; \sum_{\alpha\neq 0} f_\alpha\,(u_1,\ldots,u_l)^\alpha \;\in\; \mathfrak{u}_l$$

- Let us summarize: We have found a CPI $(0,\mathfrak{u}_1,\ldots,\mathfrak{u}_m)$ in $P_i=E[u_1,\ldots,u_m]$ and a prime ideal $\mathfrak{v}_l\trianglelefteq_{\mathfrak{i}} Q_i=A/\mathfrak{q}_{i-1}$ such that $\mathfrak{v}_l\cap P_i=\mathfrak{u}_l$. As P_i is isomorphic to a polynomial ring in m variables, it is a UFD and hence a normal domain. And as $A\neq 0$ (it is an integral domain) and E is a field, A is E-torsion-free. $Q_i\subseteq A$ inherits this property. Finally $Q_i:P_i$ is an integral extension such that we can use the going-down theorem (8.72.(iii)) to find a CPI in Q_i of the form $(\mathfrak{v}_0,\ldots,\mathfrak{v}_l)$, such that $\mathfrak{v}_j\cap P_i=\mathfrak{u}_j$ for any $j\in 0\ldots l$. By the correspondence theorem any $\mathfrak{v}_j\trianglelefteq_{\mathfrak{i}} A/\mathfrak{q}_{i-1}$ is of the form $\mathfrak{v}_j=\mathfrak{r}_j/\mathfrak{q}_{i-1}$ for some prime ideal $\mathfrak{r}_j\in A$ with $\mathfrak{q}_{i-1}\subseteq\mathfrak{r}_j$. That is we have

$$\mathfrak{q}_{i-1}\;\subseteq\;\mathfrak{r}_0\;\subset\;\mathfrak{r}_1\;\subset\;\ldots\;\subset\;\mathfrak{r}_l=\mathfrak{q}_i$$

 Hereby $\mathfrak{r}_l=\mathfrak{q}_i$ is due to the fact, that they correspond to the same ideal $\mathfrak{v}_l$ in Q_i, that is $\mathfrak{r}_l/\mathfrak{q}_{i-1}=\mathfrak{v}_l=\mathfrak{q}_l/\mathfrak{q}_{i-1}$. But the chain $(\mathfrak{q}_0,\ldots,\mathfrak{q}_r)$ was maximal, there are no prime ideals in between $\mathfrak{q}_{i-1}$ and $\mathfrak{q}_i$. That is this chain has to be $\mathfrak{q}_{i-1}=\mathfrak{r}_0\subset\mathfrak{r}_1=\mathfrak{q}_i$ and in particular $1=l=k(i)-k(i-1)$. That is $k(0)=0$ and $k(i)=k(i-1)+1$ for any $i\in 1\ldots r$. This makes $k(i)=i$ for any $i\in 1\ldots r$.

- The assumption that $(\mathfrak{q}_0,\ldots,\mathfrak{q}_r)$ is maximal also makes $\mathfrak{q}_r$ a maximal ideal. Hence $\mathfrak{q}_r\cap P$ is a maximal ideal, too, according to (8.32.(ii)). As $P=E[z_1,\ldots,z_n]$ is isomorphic to a polynomial ring in n variables, the only maximal ideal among the $z_1P+\cdots+z_kP$ is those with $k=n$. That is we have $k(r)=n$ and as we have argued above, this is $r=k(r)=n$. Thus any maximal CPI in A has length $r=n=\operatorname{trdeg}(A:E)$.

(ii) E is a field and hence noetherian. As A is finiely generated, by assumption, we recall the Hilbert basis theorem (2.42) to find that A is a noetherian ring. And any such only has finitely many prime ideals, according to (2.45.(iv)). Now use the Noetherian normalisation theorem [without a chain of ideals] (8.52) to find an an algebraically independent set $\{z_1,\ldots,z_n\}\subseteq A$ and let $P:=E[z_1,\ldots,z_n]$. As the z_i are algebraically independent, P is isomorphic to a polynomial ring $E[t_1,\ldots,t_n]$ in n variables. Thus by (8.77.(i)) we have $\operatorname{kdim}(P)=n$. But as $A:P$ is finite, it also

is integral and thereby we find by (8.73.(i))

$$\mathrm{kdim}(A) \;=\; \mathrm{kdim}(P) \;=\; n \;<\; \infty$$

As A is finite-dimensional, we may choose a CPI $(\mathfrak{q}_0,\ldots,\mathfrak{q}_n)$ of length n in A. Then the chain of quotient ideals $(\mathfrak{q}_0/\mathfrak{q}_0,\ldots,\mathfrak{q}_n/\mathfrak{q}_0)$ is a CPI in $A/\mathfrak{q}_0$ of length n again. In particular the Krull-dimension of $A/\mathfrak{q}_0$ can not be lower than n. Now use (8.69.(x)) to find the following chain of inequalities

$$n \;\leq\; \mathrm{kdim}\left(A\Big/\mathfrak{q}_0\right) \;\leq\; \mathrm{kdim}\left(A\Big/\mathfrak{q}_0\right) + \mathrm{height}(\mathfrak{q}_0) \;\leq\; \mathrm{kdim}(A) \;=\; n$$

Then we have $\mathrm{kdim}(A/\mathfrak{q}_0) = n = \mathrm{kdim}(A)$ and $\mathrm{height}(\mathfrak{q}_0) = 0$. The latter means that $\mathfrak{q}_0$ is a minimal prime ideal of A, due to (8.69.(iii)) and hence we have

$$\mathrm{kdim}(A) \;\leq\; \max\left\{\, \mathrm{kdim}\left(A\Big/\mathfrak{n}\right) \;\Big|\; \mathfrak{n} \in \mathrm{Smin}(A) \,\right\}$$

But for any prime ideal $\mathfrak{q} \trianglelefteq_{\mathrm{i}} A$ we have $\mathrm{kdim}(A/\mathfrak{q}) \leq \mathrm{kdim}(A)$ by the same reasoning - (8.69.(x)) and $\mathrm{height}(\mathfrak{q}) \geq 0$. Thus the converse inequality is a given and hence we have equality.

(iii) $A/\mathfrak{p}$ is an algebra over $E/(\mathfrak{p}\cap E)$ canonically. But as E is a field and $\mathfrak{p}\cap E \trianglelefteq_{\mathrm{i}} E$ is a proper ideal, this means $\mathfrak{p}\cap E = 0$ and hence $E/(\mathfrak{p}\cap E) = E$ canonically. Thus $A/\mathfrak{p}$ is an E-algebra, too. Also, as A is finitely generated, say $A = E[x_1,\ldots,x_n]$, so is $A/\mathfrak{p} = E[x_1+\mathfrak{p},\ldots,x_n+\mathfrak{p}]$. Thus $A/\mathfrak{p}$ is a finitely generated E-algebra and integral domain, as $\mathfrak{p}$ is prime.

Thus by (i) $A/\mathfrak{p}$ is holodimensional of dimension $\mathrm{kdim}(A/\mathfrak{p}) = \mathrm{trdeg}(A/\mathfrak{p})$. If now $\mathfrak{p} \subseteq \mathfrak{q}$ are nested primes in A, then choose a maximal ideal $\mathfrak{m} \trianglelefteq_{\mathrm{i}} A$ such that $\mathfrak{q} \trianglelefteq_{\mathrm{i}} \mathfrak{m}$. Then $(\mathfrak{p},\mathfrak{q},\mathfrak{m})$ is a CPI in A - if $\mathfrak{p}=\mathfrak{q}$ or $\mathfrak{q}=\mathfrak{m}$ just omit one of the duplicates. By the correspondence theorem

$$0 \;=\; \mathfrak{p}\Big/\mathfrak{p} \;\subseteq\; \mathfrak{q}\Big/\mathfrak{p} \;\subseteq\; \mathfrak{m}\Big/\mathfrak{p}$$

is a CPI in $A/\mathfrak{p}$ (except for duplicates). As $\mathrm{kdim}(A/\mathfrak{p}) \leq \mathrm{kdim}(A) < \infty$ we can append this chain to a maximal CPI in $A/\mathfrak{p}$. Let $(\mathfrak{u}_0,\ldots,\mathfrak{u}_r,\ldots,\mathfrak{u}_m)$ be that CPI, where $\mathfrak{u}_0 = \mathfrak{p}/\mathfrak{p}$, $\mathfrak{u}_r = \mathfrak{q}/\mathfrak{p}$ and $\mathfrak{u}_m = \mathfrak{m}/\mathfrak{p}$. In particular $(\mathfrak{u}_0,\ldots,\mathfrak{u}_r)$ is saturated and thereby uniquely determined to be

$$r \;=\; \mathrm{kdim}\left(A\Big/\mathfrak{p}\right) - \mathrm{kdim}\left(A\Big/\mathfrak{q}\right)$$

by (8.75.(ii)). Conversely, if $(\mathfrak{q}_0,\ldots,\mathfrak{q}_s)$ another saturated CPI of A with $\mathfrak{q}_0=\mathfrak{p}$ and $\mathfrak{q}_s=\mathfrak{q}$, then (8.75.(ii)) also tells us $s=r$. That is there is a CPI connecting $\mathfrak{p}$ and $\mathfrak{q}$ and the length of any such sturated chain, is uniquely determined. In other words A is catenary.

(iv) The first part $\mathrm{kdim}(A) = n$ has already been proved in (ii). We go a little further: As $\{\, z_1,\ldots,z_n \,\}$ is algebraically independent $P = E[z_1,\ldots,z_n]$ is isomorphic to a polynomial ring in n variables over E. But as such it even is an UFD - by the lemma of Gauss (7.29.(iv)) - and hence a normal domain - due to (2.65). We will require this for the proof of $\mathrm{height}(\mathfrak{a}_i) = k(i)$ for any $i \in 1\ldots r$:

For any $k \in 0\ldots n$ let us denote $\mathfrak{p}_k := z_1P + \cdots + z_kP \trianglelefteq_{\mathrm{i}} P$. That is $\mathfrak{p}_k$ is the ideal generated by $\{\, z_1,\ldots,z_k \,\}$. And therefore we have $\mathrm{height}(\mathfrak{p}_k) = k$ by (8.77.(ii)). Yet as $A:P$ is finite, it also

is integral and P is a normal domain, as we have argued above. And as A is an integral domain it also is torsion-free, as a P-module. Therefore we can invoke (8.73.(iv)) to find the desired identity

$$\text{height}\big(\mathfrak{a}_i\big) \;=\; \text{height}\big(\mathfrak{a}_i \cap P\big) \;=\; \text{height}\big(\mathfrak{p}_{k(i)}\big) \;=\; k(i)$$

□

Proof of (8.78):

(i) As A is an E-algebra, so is $A_\mathfrak{p}$ under $a(f/u) = (af)/u$. And therefore the quotient $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ is an E-algebra, too. Also note that due to (2.138) we have the following isomorphy

$$E_\mathfrak{p} \;=\; A_\mathfrak{p}\Big/_{\mathfrak{p}A_\mathfrak{p}} \;\xrightarrow{\sim}\; \text{QUOT}\left(A\Big/_\mathfrak{p}\right) \;:\; \frac{f}{u} + \mathfrak{p}A_\mathfrak{p} \mapsto \frac{f+\mathfrak{p}}{u+\mathfrak{p}}$$

And as $\mathfrak{p}$ is a prime ideal $A/\mathfrak{p}$ is an integral domain, such that $\text{kdim}(A/\mathfrak{p}) = \text{trdeg}(A/\mathfrak{p} : E)$ because of (8.76.(i)). But the transcendence degree remains unchanged, when going to quotient fields, due to (8.49.(ii)). Then we finally use the isomorphisms of $E_\mathfrak{p}$ and $E = \text{QUOT}(E)$ to find the following identity, in the end:

$$\text{kdim}\left(A\Big/_\mathfrak{p}\right) \;=\; \text{trdeg}\left(A\Big/_\mathfrak{p} : E\right) \;=\; \text{trdeg}\left(\text{QUOT}\left(A\Big/_\mathfrak{p}\right) : \text{QUOT}(E)\right) \;=\; \text{trdeg}(E_\mathfrak{p} : E)$$

(ii) Consider a minimal prime ideal $\mathfrak{p}_* \in \text{Smin}(A)$ such that $\mathfrak{p}_* \subseteq \mathfrak{p}$ and append $(\mathfrak{p}_*, \mathfrak{p})$ to a maximal CPI $(\mathfrak{p}_0, \ldots, \mathfrak{p}_r)$ of A. As $\mathfrak{p}_*$ is a minimal prime ideal, we have $\mathfrak{p}_0 = \mathfrak{p}_*$. Then by (8.76.(iii)) we find

$$r \;=\; \text{kdim}\left(A\Big/_{\mathfrak{p}_*}\right) - \text{kdim}\left(A\Big/_{\mathfrak{p}_r}\right)$$

Also $\mathfrak{p}_r$ is a maximal ideal, as the CPI, was maximal, thus $A/\mathfrak{p}_r$ is a field. In particular the Krull-dimension of $A/\mathfrak{p}_r$ is 0 and hence the above equality turns into

$$\text{kdim}\left(A\Big/_{\mathfrak{p}_*}\right) \;=\; r \;\leq\; \sup\left\{ \ell(\mathcal{P}) \;\middle|\; \begin{array}{l} \mathcal{P} \in \text{CPI}(A) \\ \text{with } \mathfrak{p} \in \mathcal{P} \end{array} \right\}$$

As this is true for any minimal prime ideal $\mathfrak{p}_*$ contained in $\mathfrak{p}$ this already means that the maximal Krull dimension of $A/\mathfrak{p}_*$ cannot exceed the supremum of the length of chains containing $\mathfrak{p}$

$$\max\left\{ \text{kdim}\left(A\Big/_{\mathfrak{p}_*}\right) \;\middle|\; \begin{array}{l} \mathfrak{p}_* \in \text{Smin}(A) \\ \text{with } \mathfrak{p}_* \subseteq \mathfrak{p} \end{array} \right\} \;\leq\; \sup\left\{ \ell(\mathcal{P}) \;\middle|\; \begin{array}{l} \mathcal{P} \in \text{CPI}(A) \\ \text{with } \mathfrak{p} \in \mathcal{P} \end{array} \right\}$$

Conversely let $\mathcal{P} = (\mathfrak{p}_0, \ldots, \mathfrak{p}_r)$ be a CPI of A containing $\mathfrak{p} \in \mathcal{P}$. As we need to control the length of $\mathcal{P}$ anyway, we may assume $\mathcal{P}$ to be maximal already. Thus $\mathfrak{p}_0 \in \text{Smin}(A)$ is a minimal ideal and $\mathfrak{p} \in \mathcal{P}$ this yields $\mathfrak{p}_0 \subseteq \mathfrak{p}$. By going to quotients $/\mathfrak{p}_0$ we turn to

$$0 \;=\; \mathfrak{p}_0\Big/_{\mathfrak{p}_0} \;\subset\; \mathfrak{p}_1\Big/_{\mathfrak{p}_0} \;\subset\; \ldots \;\subset\; \mathfrak{p}_r\Big/_{\mathfrak{p}_0}$$

which is a (maximal) CPI in $A/\mathfrak{p}_0$ of length r. In particular its length r cannot exceed $\text{kdim}(A/\mathfrak{p}_0)$

and therefore we also have the converse inequality and therefore

$$\max\left\{ \operatorname{kdim}\left(A\Big/\mathfrak{p}_*\right) \;\middle|\; \begin{array}{l}\mathfrak{p}_* \in \operatorname{Smin}(A)\\ \text{with } \mathfrak{p}_* \subseteq \mathfrak{p}\end{array} \right\} \;=\; \sup\left\{ \ell(\mathcal{P}) \;\middle|\; \begin{array}{l}\mathcal{P} \in \operatorname{CPI}(A)\\ \text{with } \mathfrak{p} \in \mathcal{P}\end{array} \right\}$$

- It remains to prove, that this also equals $\operatorname{kdim}(A/\mathfrak{p}) + \operatorname{height}(\mathfrak{p})$: Thus consider any CPI $\mathcal{P} = (\mathfrak{p}_0, \ldots, \mathfrak{p}_r)$ of A such that $\mathfrak{p} \in \mathcal{P}$ and $\mathcal{P}$ is of maximal length, with this property. Say $\mathfrak{p} = \mathfrak{p}_k$ for some $k \in 0 \ldots n$. In particular $\mathfrak{p}_r$ is a maximal ideal, else we could append a maximal ideal containing $\mathfrak{p}_r$ to obtain a CPI of length $r+1$, also containing $\mathfrak{p}$. This is impossible, as we chose r to be maximal. Then $A/\mathfrak{p}_r$ is a field and hence $\operatorname{kdim}(A/\mathfrak{p}_r) = 0$ again, such that by (8.76.(iii))

$$\operatorname{kdim}\left(A\Big/\mathfrak{p}\right) \;=\; \operatorname{kdim}\left(A\Big/\mathfrak{p}_k\right) - \operatorname{kdim}\left(A\Big/\mathfrak{p}_r\right) \;=\; r-k$$

 That is $\operatorname{kdim}(A/\mathfrak{p}) + k = r$. As $(\mathfrak{p}_0, \ldots, \mathfrak{p}_k)$ is a CPI ending in $\mathfrak{p} = \mathfrak{p}_k$ we have $k \leq \operatorname{height}(\mathfrak{p})$. Suppose we had $k < \operatorname{height}(\mathfrak{p})$, that is there was SOME CPI $(\mathfrak{q}_0, \ldots, \mathfrak{q}_m)$ such that $\mathfrak{q}_m = \mathfrak{p}$ and $m > k$. But this would mean that $(\mathfrak{q}_0, \ldots, \mathfrak{q}_m, \mathfrak{p}_{k+1}, \ldots, \mathfrak{p}_r)$ would be a CPI of length $r + m - k > r$ containing $\mathfrak{p}$, contradicting the maximality of r, again. Thus we have $k = \operatorname{height}(\mathfrak{p})$ and hence $r = \operatorname{kdim}(A/\mathfrak{p}) + \operatorname{height}(\mathfrak{p})$. And as r was the supremum, the third equality is established.

(iii) Let us first check (1), that $\{\, \overline{z}_{k+1}, \ldots, \overline{z}_n \,\}$ are algebraically independent. That is we regard any polynomial $f \in E[t_{k+1}, \ldots, t_n]$ such that $f(\overline{z}_{k+1}, \ldots, \overline{z}_n) = 0 + \mathfrak{p}$. As $x \mapsto \overline{x}$ is a homomorphism of E-algebras, this means $f(z_{k+1}, \ldots, z_n) + \mathfrak{p} = 0 + \mathfrak{p}$ and hence $f(z_{k+1}, \ldots, z_n) \in \mathfrak{p}$. As also $f(z_{k+1}, \ldots, z_n) \in E[z_1, \ldots, z_n] = P$ we then get

$$f(z_{k+1}, \ldots, z_n) \;\in\; \mathfrak{p} \cap P \;=\; z_1 P + \cdots + z_k P$$

 That is $f(z_{k+1}, \ldots, z_n) \in E[z_{k+1}, \ldots, z_n] \cap E[z_1, \ldots, z_k] = E$. As f cannot be constant $f \in E^*$ there only remains $f = 0$, which is the algebraic independence of $\{\, \overline{z}_{k+1}, \ldots, \overline{z}_n \,\}$.

- Let us prove (4) next: Note that the canonical epimorphism $\varrho : A \twoheadrightarrow A/\mathfrak{p} : x \mapsto x + \mathfrak{p}$ maps $\varrho(z_j) = 0 + \mathfrak{p}$ for $j \in 1 \ldots k$, as $z_j \in \mathfrak{p} \cap P \subseteq \mathfrak{p}$ and $\varrho(z_j) = \overline{z}_j$ for $j \in k+1 \ldots n$, by construction. Thus, for any element $f(z_1, \ldots, z_n) \in P$ we find

$$f(z_1, \ldots, z_n) + \mathfrak{p} \;=\; f\big(0, \ldots, 0, \overline{z}_{k+1}, \ldots, \overline{z}_n\big)$$

 In particular $\varrho(P) = E[\overline{z}_{k+1}, \ldots, \overline{z}_n]$. Let us take a look at the kernel of ϱ in P: From the above identity it is clear, that $f(z_1, \ldots, z_n) + \mathfrak{p} = 0$ iff $f(z_1, \ldots, z_n) \in z_1 P + \cdots + z_k P = \mathfrak{p} \cap P$. That is the restriction of ϱ to P induces the desired isomorphism, by the first isomorphism theorem

$$P\Big/\mathfrak{p} \cap P \;\xrightarrow{\sim}\; E[\overline{z}_{k+1}, \ldots, \overline{z}_n] \;:\; f(z_1, \ldots, z_n) + \mathfrak{p} \cap P \mapsto f(z_1, \ldots, z_n) + \mathfrak{p}$$

- For property (2) we note, that $A : P$ is finite and by (4) we know $\varrho(P) = E[\overline{z}_{k+1}, \ldots, \overline{z}_n] = \overline{P}$. Therefore we can conclude that $A/\mathfrak{p} : \overline{P}$ is finite, by (8.28). And now, that $A/\mathfrak{p} : \overline{P}$ is finite, it also is integral. Thus we have $\operatorname{kdim}(A/\mathfrak{p}) = \operatorname{kdim}(\overline{P})$, according to (8.73.(i)). But as $\{\, \overline{z}_{k+1}, \ldots, \overline{z}_n \,\}$ is algebraically independent $\overline{P}$ is isomorphic to a polynomial ring in $n-k$ variables over the field E and hence $\operatorname{kdim}(A/\mathfrak{p}) = \operatorname{kdim}(\overline{P}) = n - k$.

- It remains to prove (5): As for any $j \in 1 \ldots k$ we have $z_j \in \mathfrak{p} \cap P \subseteq \mathfrak{a}_1 \cap P = z_1 P + \cdots + z_{k(1)} P$ we conclude $j \leq k(i)$, as the $z_1 P + \cdots + z_i P$ form a CPI in P. Therefore $k \leq k(1)$. And for $j \in k+1 \ldots k(i)$ we have $z_j \in z_j P \subseteq \mathfrak{a}_i \cap P$ such that $\overline{z}_j = z_j + \mathfrak{p} = \varrho(z_j) \in (\mathfrak{a}_i/\mathfrak{p}) \cap \varrho(P)$ where $\varrho(P) = \overline{P}$, as we have seen in (4). Thus we have found the inclusion

$$\overline{z}_{k+1}\overline{P} + \cdots + \overline{z}_{k(i)}\overline{P} \quad \subseteq \quad \mathfrak{a}_i \Big/ \mathfrak{p} \cap \overline{P}$$

In the converse direction we start with some some $\overline{x} = x + \mathfrak{p} \in \mathfrak{a}_i/\mathfrak{p} \cap \overline{P}$. That is $x \in \mathfrak{a}_i$ and $x + \mathfrak{p} = \varrho(x) \in \overline{P} = \varrho(P)$. The latter is $x \in P$ and thereby $x \in \mathfrak{a}_i \cap P = z_1 P + \cdots + z_{k(i)} P$ by assumption. But then $\varrho(x) \in \sum_j \varrho(z_j)\overline{P}$ and we have already seen $\varrho(z_j) = 0$ for $j \in 1 \ldots k$. Thus it only remains $x + \mathfrak{p} = \varrho(x) \in \sum_j \varrho(z_j)\overline{P}$ where the sum runs from $j = k+1$ to $j = n$. Thus we also have the converse inclusion.

□

Proof of (8.79):

(i) From the definition it is clear, that $\operatorname{trdeg}(A : E) \leq \operatorname{tfree}(A : E)$, as any transcendence basis $U \subseteq A$ already has to be algebraically independent. Now let $U \subseteq A$ be be any algebraically independent set. As A is an integral domain, we find a transcendence basis $V \subseteq A$ with $U \subseteq V$, according to (8.47.(i)). In particular $\#U \leq \#V = \operatorname{trdeg}(A : E)$ and thereby $\operatorname{tfree}(A : E) \leq \operatorname{trdeg}(A : E)$, too.

(ii) As $\mathfrak{q} \trianglelefteq_{\mathfrak{i}} A$ is prime, $A/\mathfrak{q}$ is an integral domain. Hence we may choose a transcendence basis of $A/\mathfrak{q} : E$, say $\{ u_i + \mathfrak{q} \mid i \in I \} \subseteq a/\mathfrak{q}$. Then we let $U := \{ u_i \mid i \in I \}$ and claim, that U is algebraically independent. Consider any $u_1, \ldots, u_n \in U$ and some polynomial $f \in E[t_1, \ldots, t_n]$ such that $f(u_1, \ldots, u_n)$, then we also get

$$f(u_1 + \mathfrak{q}, \ldots, u_n + \mathfrak{q}) \;=\; f(u_1, \ldots, u_n) + \mathfrak{q} \;=\; 0 + \mathfrak{q}$$

But as the $u_i + \mathfrak{q}$ are algebraically independent, we conclude $f = 0$ from this equality. And thereby $\{ u_1, \ldots, u_n \}$ is algebraically independent. As this is true for any finite subset, U itself is algebraically independent. And thereby $\operatorname{tfree}(A/\mathfrak{q} : E) = \operatorname{trdeg}(A/\mathfrak{q} : E) = \#I \leq \operatorname{tfree}(A : E)$.

(iii) This proof will take several steps: First of all, let A be a finite-dimensional integral domain. Then we pick up a CPI $\mathfrak{q}_0 \subset \ldots \subset \mathfrak{q}_r$ in A of length $r = \operatorname{kdim}(A)$. As the inclusions are strict, we can pick some elements $x_i \in A$ such that

$$x_i \quad \in \quad \mathfrak{q}_i \setminus \mathfrak{q}_{i-1}$$

for any $i \in 1 \ldots r$. Now let $P := E[x_1, \ldots, x_r] \subseteq A$. As A is an integral domain, so is P. And by construction P is finitely generated. Thus we get from (8.76.(i)) and (i) we get

$$\operatorname{kdim}(P) \;=\; \operatorname{trdeg}(P : E) \;=\; \operatorname{tfree}(P : E)$$

Now let $\mathfrak{p}_i := \mathfrak{q}_i \cap P$, then it is clear that these ideals form an ascending chain $\mathfrak{p}_0 \subseteq \ldots \subseteq \mathfrak{p}_r$. But as $x_i \in \mathfrak{q}_i \cap P = \mathfrak{p}_i$ though $x_i \notin \mathfrak{q}_{i-1}$ we find that these inclusions are strict $\mathfrak{p}_0 \subset \ldots \subset \mathfrak{p}_r$

even. In particular the Krull-dimension of P is r at least

$$r \;\leq\; \mathrm{kdim}(P) \;=\; \mathrm{trdeg}(P:E)$$

As $E[t_1,\ldots,t_r] \twoheadrightarrow P$ we even get $\mathrm{kdim}(P) = r$, but we actually do not need this here. Recall that we took $r = \mathrm{kdim}(A)$. And as all E, P and A are integral domains we have (8.49.(iii)) which yields the desired inequality

$$\mathrm{kdim}(A) \;=\; r \;=\; \mathrm{trdeg}(P:E) \;\leq\; \mathrm{trdeg}(A:P) + \mathrm{trdeg}(P:E) \;=\; \mathrm{trdeg}(A:E)$$

- If A is an integral domain with $\mathrm{kdim}(A) = \infty$, then there are CPI of unbound length r in A. And by the construction above, this can be turned into $r \leq \mathrm{trdeg}(A:E)$. Thus $\mathrm{trdeg}(A:E)$ is unbound, too and hence $\mathrm{trdeg}(A:E) = \infty = \mathrm{kdim}(A)$.

- Now consider a finite-dimensional E-algebra A, that may contain zero-divisors. Again let $\mathfrak{q}_0 \subset \ldots \subset \mathfrak{q}_r$ be a CPI in A with $r = \mathrm{kdim}(A)$. By the correspondence theorem (8.65.(i)) we get the CPI $0 = \mathfrak{q}_0/\mathfrak{q}_0 \subset \ldots \subset \mathfrak{q}_r/\mathfrak{q}_0$ in $A/\mathfrak{q}_0$ and thereby $\mathrm{kdim}(A\mathfrak{q}_0) \geq r$. But also $\mathrm{kdim}(A/\mathfrak{q}_0) \leq \mathrm{kdim}(A) = r$ by (8.69.(x)). Together this is $\mathrm{kdim}(A/\mathfrak{q}_0) = r = \mathrm{kdim}(A)$. But $A/\mathfrak{q}_0$ is an integral domain, too, such by the step above and (ii) we can conclude

$$\mathrm{kdim}(A) \;=\; r \;=\; \mathrm{kdim}\left(A\Big/\mathfrak{q}_0\right) \;\leq\; \mathrm{tfree}\left(A\Big/\mathfrak{q}_0 : E\right) \;\leq\; \mathrm{tfree}(A:E)$$

- Let finally A be an E-algebra of $\mathrm{kdim}(A) = \infty$, that may contain zero-divisors. then there are CPI of unbound length r in A. And by the construction above, this can be turned into $r \leq \mathrm{tfree}(A:E)$. Thus $\mathrm{tfree}(A:E)$ is unbound, too and hence $\mathrm{tfree}(A:E) = \infty = \mathrm{kdim}(A)$.

(iv) By (iii) we know $\mathrm{kdim}(P) \leq \mathrm{tfree}(P:E)$ and as $P \subseteq A$ any algebraically independent $U \subseteq P$ also is an algebraically subset $U \subseteq A$. Thus we have $\mathrm{tfree}(P:E) \leq \mathrm{tfree}(A:E)$. But as A is an integral domain we have $\mathrm{free}(A:E) = \mathrm{trdeg}(A:E)$ and as A also is finitely generated by (8.76.(i)) $\mathrm{trdeg}(A:E) = \mathrm{kdim}(A)$. Altogether that is

$$\mathrm{kdim}(P) \;\leq\; \mathrm{tfree}(P:E) \;\leq\; \mathrm{tfree}(A:E) \;=\; \mathrm{trdeg}(A:E) \;=\; \mathrm{kdim}(A)$$

□

Proof of (8.80):

(i) **Claim:** Let R be a noetherian, local integral domain with maximal ideal $\mathfrak{p}$. Also let $a \in R$ be an element with $a \neq 0$ and $\mathfrak{p}$ also is a minimal prime ideal over aR. Then $\mathrm{height}(\mathfrak{p}) = 1$, that is: If $\mathfrak{p}_0 \in \mathrm{Spec}(R)$ is another prime ideal satisfying $0 \subseteq \mathfrak{p}_1 \subset \mathfrak{p}$, then we already have $\mathfrak{p}_1 = 0$.

- **Proof:** By assumption $\mathfrak{p}$ is the one and only maximal ideal of R and hence $\mathrm{JAC}(R) = \mathfrak{p}$. Also $\mathfrak{p}$ is a minimal prime ideal over $\mathfrak{a} := aR \trianglelefteq_{\mathrm{i}} R$. Suppose we had $a \in \mathfrak{p}_1$ then $\mathfrak{a} \subseteq \mathfrak{p}_1 \subset \mathfrak{p}$. As $\mathfrak{p}$ is minimal over $\mathfrak{a}$ we would get $\mathfrak{p}_1 = \mathfrak{p}$, which is untrue. Therefore we find $a \notin \mathfrak{p}_1$.

 Now take to the quotient ring $R/\mathfrak{a}$. We will argue, that $R/\mathfrak{a}$ has one and one prime ideal only $\mathrm{Spec}(R/\mathfrak{a}) = \{\,\mathfrak{p}/\mathfrak{a}\,\}$: Consider any prime ideal $\mathfrak{u}$ of $R/\mathfrak{a}$. Then $\mathfrak{u}$ is of the form $\mathfrak{u} = \mathfrak{p}'/\mathfrak{a}$ for

some $\mathfrak{p}' \in \mathrm{Spec}(R)$ with $\mathfrak{a} \subseteq \mathfrak{p}'$. But as $\mathfrak{p}' \neq R$ is a proper ideal, it is contained in a maximal ideal, by (2.4.(ii)). But the only maximal ideal available in R is $\mathfrak{p}$ such that we get $\mathfrak{a} \subseteq \mathfrak{p}' \subseteq \mathfrak{p}$. As $\mathfrak{p}$ is minimal over $\mathfrak{a}$ we conclude $\mathfrak{p}' = \mathfrak{p}$ again. In particular

$$\mathrm{kdim}\left(R \Big/ \mathfrak{a}\right) \;=\; 0$$

as we don't even have a second prime ideal to build a chain with. But as quotients of a noetherian ring R are noetherian again, so is $R/\mathfrak{a}$. But zero-dimensional noetherian rings are artinian, by (2.37.(e)). We now make use of the *symbolic powers* $\mathfrak{p}_1^{(n)}$ of $\mathfrak{p}_1$. As $R/\mathfrak{a}$ is artinian the following descending chain of ideals in R

$$\mathfrak{p}_1^{(0)} + \mathfrak{a} \;\supseteq\; \mathfrak{p}_1^{(1)} + \mathfrak{a} \;\supseteq\; \mathfrak{p}_1^{(2)} + \mathfrak{a} \;\supseteq\; \mathfrak{p}_1^{(3)} + \mathfrak{a} \;\supseteq\; \ldots$$

has to stabilize, as it corresponds to a chain of ideals in $R/\mathfrak{a}$. That is there is some $n \in \mathbb{N}$ such that $\mathfrak{p}_1^{(n+1)} + \mathfrak{a} = \mathfrak{p}_1^{(n)} + \mathfrak{a}$. In particular $\mathfrak{p}_1^{(n)} \subseteq \mathfrak{p}_1^{(n+1)} + \mathfrak{a} = \mathfrak{p}_1^{(n+1)} + aR$. In the next step we will prove that for this n we get the identity

$$\mathfrak{p}_1^{(n)} \;=\; \mathfrak{p}_1^{(n+1)} + \mathfrak{p}\,\mathfrak{p}_1^{(n)}$$

- As both $\mathfrak{p}_1^{(n+1)} \subseteq \mathfrak{p}_1^{(n)}$ and $\mathfrak{p}\,\mathfrak{p}_1^{(n)} \subseteq \mathfrak{p}_1^{(n)}$ the inclusion from right to left is clear. For the converse inclusion we start with any $p \in \mathfrak{p}_1^{(n)}$. As we already have $\mathfrak{p}_1^{(n)} \subseteq \mathfrak{p}_1^{(n+1)} + aR$ there are some elements $q \in \mathfrak{p}_1^{(n+1)}$ and $r \in R$ such that $p = q + ar$. In particular $q \in \mathfrak{p}_1^{(n+1)} \subseteq \mathfrak{p}_1^{(n)}$ such that $ar = p - q \in \mathfrak{p}_1^{(n)}$. But by (2.92.(iii)) $\mathfrak{p}_1^{(n)}$ is a $\mathfrak{p}_1$ primary ideal. And as $ar \in \mathfrak{p}_1^{(n)}$ but $a \notin \mathfrak{p}_1 = \sqrt{\mathfrak{p}_1^{(n)}}$ we hence get $r \in \mathfrak{p}_1^{(n)}$. That is we have $p = q + ar \in \mathfrak{p}_1^{(n+1)} + \mathfrak{p}\,\mathfrak{p}_1^{(n)}$ since $a \in \mathfrak{p}$. And this is the inclusion from left to right.
- Consider $M := \mathfrak{p}_1^{(n)}$ as an R-module and $P := \mathfrak{p}_1^{(n+1)}$ a sub-module of M. As R is noetherian, M is finitely generated and we have just proved $M = P + \mathfrak{p}M$. Recall $\mathfrak{p} = \mathrm{JAC}(R)$, then the lemma of Nakayama (3.44.(iii)) tells us $P = M$, that is $\mathfrak{p}_1^{(n+1)} = \mathfrak{p}_1^{(n)}$. Then we can use (2.92.(iv)) to compute

$$\mathfrak{p}_1^n\, R_{\mathfrak{p}_1} \;=\; \mathfrak{p}_1^{(n)}\, R_{\mathfrak{p}_1} \;=\; \mathfrak{p}_1^{(n+1)}\, R_{\mathfrak{p}_1} \;=\; \mathfrak{p}_1^{n+1}\, R_{\mathfrak{p}_1}$$

 But by (8.21.(ii)) we also have $\mathfrak{p}_1^{n+1}\, R_{\mathfrak{p}_1} = \big(\mathfrak{p}_1\mathfrak{p}_1^n\big) R_{\mathfrak{p}_1} = \big(\mathfrak{p}_1\, R_{\mathfrak{p}_1}\big)\big(\mathfrak{p}_1^n\, R_{\mathfrak{p}_1}\big)$. Note that $R_{\mathfrak{p}_1}$ is a local ring with maximal ideal $\mathfrak{j} := \mathfrak{p}_1\, R_{\mathfrak{p}_1}$ - that is this ideal also is the Jacobson-radical of $R_{\mathfrak{p}_1}$. So if we consider the ideal $M := \mathfrak{p}_1^n\, R_{\mathfrak{p}_1}$ as an R-module again, we have $M = \mathfrak{p}_1^{n+1}\, R_{\mathfrak{p}_1} = \mathfrak{j}M$, such that another dose of the lemma of Nakayama (3.44.(ii)) leaves us with $\mathfrak{p}_1^n\, R_{\mathfrak{p}_1} = M = 0$.
- Now suppose we had $\mathfrak{p}_1 \neq 0$, that is there is some $p \in \mathfrak{p}_1$ with $p \neq 0$. Then we had $p^n \in \mathfrak{p}_1^n$ and as R is an integral domain, also $p^n \neq 0$. Therefore $p^n/1 \in \mathfrak{p}_1^n\, R_{\mathfrak{p}_1}$ also is $p^n/1 \neq 0/1$ non-zero, as $up^n = 0$ would mean $0 = u \in R \setminus \mathfrak{p}_1$. But this contradicts $\mathfrak{p}_1^n\, R_{\mathfrak{p}_1} = 0$, such we have to settle with $\mathfrak{p}_1 = 0$ and this has been claimed, above.
- **Proof** of (i) in general: We have to show $\mathrm{height}(\mathfrak{p}) \leq 1$, so consider a CPI $(\mathfrak{p}_0, \ldots, \mathfrak{p}_r)$ of R with $\mathfrak{p}_r = \mathfrak{p}$. If $a \in \mathfrak{p}_0$ there is not much to do: As $aR \subseteq \mathfrak{p}_0 \subseteq \mathfrak{p}$ and $\mathfrak{p}$ is minimal over aR we have $\mathfrak{p}_0 = \mathfrak{p}$ and thereby $r = 0$. Such a chain is of length 0. In case $a \notin \mathfrak{p}_0$ we continue: Consider the setup $\mathfrak{p}_0 \subseteq \mathfrak{p}_1 \subset \mathfrak{p}$, then we will prove $\mathfrak{p}_0 = \mathfrak{p}_1$. From this we conclude that the above CPI

can be $(\mathfrak{p}_0, \mathfrak{p}_1)$ with $\mathfrak{p}_1 = \mathfrak{p}$ at most and hence $r \leq 1$ in this case. In both cases we then have height$(\mathfrak{p}) \leq 1$, which is the claim.

As $a \in \mathfrak{p}_0$ is done with, we regard $a \notin \mathfrak{p}_0$. In this case we take to the quotient ring $Q := R/\mathfrak{p}_0$ which is an integral domain and clearly is noetherian again - if $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$ is generated by $\mathfrak{a} = \langle a_1, \ldots, a_n \rangle_{\mathfrak{i}}$ and $\mathfrak{p} \subseteq \mathfrak{a}$, then $\mathfrak{a}/\mathfrak{p}$ is generated by $\langle a_1 + \mathfrak{p}, \ldots, a_n + \mathfrak{p} \rangle_{\mathfrak{i}}$. The chain $\mathfrak{p}_0 \subseteq \mathfrak{p}_1 \subset \mathfrak{p}$ then turns into the following chain in Q

$$0 \;=\; \mathfrak{p}_0 \Big/ \mathfrak{p}_0 \;\subseteq\; \mathfrak{p}_1 \Big/ \mathfrak{p}_0 \;\subset\; \mathfrak{p} \Big/ \mathfrak{p}_0$$

Let us abbreviate $\overline{\mathfrak{p}} := \mathfrak{p}/\mathfrak{p}_0$. As $a \notin \mathfrak{p}_0$ we have $0 \neq a + \mathfrak{p}_0 \in \overline{\mathfrak{p}}$ such that $\overline{\mathfrak{p}} \neq 0$ is non-zero. Now we continue to $Q_{\overline{\mathfrak{p}}}$ which is a local ring by (2.138) and a noetherian integral domain by (2.131). And the above chain turns into a chain of prime ideals in $Q_{\overline{\mathfrak{p}}}$

$$0 \;=\; \mathfrak{p}_0 \Big/ \mathfrak{p}_0 Q_{\overline{\mathfrak{p}}} \;\subseteq\; \mathfrak{p}_1 \Big/ \mathfrak{p}_0 Q_{\overline{\mathfrak{p}}} \;\subset\; \mathfrak{p} \Big/ \mathfrak{p}_0 Q_{\overline{\mathfrak{p}}}$$

Again, as $\overline{a} := a + \mathfrak{p} \neq 0 + \mathfrak{p}$ we get $\overline{a}/\overline{1} \neq \overline{0}/\overline{1}$. Suppose there was a prime ideal in between $\overline{a}/\overline{1}\, Q_{\overline{\mathfrak{p}}}$ and $\overline{\mathfrak{p}}\, Q_{\overline{\mathfrak{p}}}$. Then by (8.65.(iii)) this prime ideal would correspond to a prime ideal $\mathfrak{p}'$ in R, strictly underneath $\mathfrak{p}$. This ideal would be of the form $\overline{\mathfrak{p}}'\, Q_{\overline{\mathfrak{p}}}$ for some $\mathfrak{p}' \in \operatorname{Spec}(R)$. And as $\overline{a}/\overline{1} \in \overline{\mathfrak{p}}'\, Q_{\overline{\mathfrak{p}}}$ we had $\overline{a} \in \overline{\mathfrak{p}}'$ and thereby $a \in \mathfrak{p}'$. That is we had the chain $aR \subseteq \mathfrak{p}' \subset \mathfrak{p}$, but as $\mathfrak{p}$ is a minimal prime ideal over aR, there is no such $\mathfrak{p}'$ and hence $\overline{\mathfrak{p}}\, Q_{\overline{\mathfrak{p}}}$ is a minimal prime ideal over $\overline{a}/\overline{1}\, Q_{\overline{\mathfrak{p}}}$.

Now $Q_{\overline{\mathfrak{p}}}$ and $\overline{\mathfrak{p}}\, Q_{\overline{\mathfrak{p}}}$ satisfy the properties required in the claim above. Looking at the chain of prime ideals in $Q_{\overline{\mathfrak{p}}}$ above, we conclude that $\mathfrak{p}_1/\mathfrak{p}_0\, Q_{\overline{\mathfrak{p}}} = 0$. But this means $\mathfrak{p}_1/\mathfrak{p}_0 = 0$ by the correspondence theorem (2.129) which is the claim we needed: We have arrived, at $\mathfrak{p}_0 = \mathfrak{p}_1$ from which we conclude $r \leq 1$.

(iv) Let us conduct this proof by induction on r: For $r = 1$ there is nothing to prove, the claim equals the assumption. So let us consider the case $r = 2$: If $a \in \mathfrak{p}_1$ already, then we are done. Else take to the quotient ring $Q := R/\mathfrak{p}_0$ and regard the chain

$$0 \;=\; \mathfrak{p}_0 \Big/ \mathfrak{p}_0 \;\subset\; \mathfrak{p}_1 \Big/ \mathfrak{p}_0 \;=\; \mathfrak{p}_2 \Big/ \mathfrak{p}_0$$

We have $(a + \mathfrak{p}_0)Q \subseteq \mathfrak{p}_2/\mathfrak{p}_0$ by assumption and hence there is a prime ideal, minimal over $(a + \mathfrak{p}_0)Q$ contained in $\mathfrak{p}_2/\mathfrak{p}_0$, according to (2.18.(iv)). This ideal is of the form $\widetilde{\mathfrak{p}}_1/\mathfrak{p}_0$ for some prime ideal $\widetilde{\mathfrak{p}}_1$ of R with $\mathfrak{p}_0 \subseteq \widetilde{\mathfrak{p}}_1$. As $\widetilde{\mathfrak{p}}_1/\mathfrak{p}_0 \subseteq \mathfrak{p}_2/\mathfrak{p}_0$ we get $\widetilde{\mathfrak{p}}_1 \subseteq \mathfrak{p}_2$ so by now we have

$$\mathfrak{p}_0 \;\subseteq\; \widetilde{\mathfrak{p}}_1 \;\subseteq\; \mathfrak{p}_2$$

Clearly $a \in \widetilde{\mathfrak{p}}_1$ as $a + \mathfrak{p}_0 \in \widetilde{\mathfrak{p}}_1/\mathfrak{p}_0$. And as $a + \mathfrak{p}_0 \neq 0 + \mathfrak{p}_0$ we have $a \in \widetilde{\mathfrak{p}}_1 \setminus \mathfrak{p}_0$ such that $\mathfrak{p}_0 \subset \widetilde{\mathfrak{p}}_1$. And as $\widetilde{\mathfrak{p}}_1/\mathfrak{p}_0$ is minimal over $(a + \mathfrak{p}_0)Q$ we have height$(\widetilde{\mathfrak{p}}_1/\mathfrak{p}_0) \leq 1$, as we have just proved in (i). But height$(\mathfrak{p}_2/\mathfrak{p}_0) \geq 2$, as we startet with a chain of length 2, Thus we also have $\widetilde{\mathfrak{p}}_1 \neq \mathfrak{p}_2$ which amounts to $\widetilde{\mathfrak{p}}_1 \subset \mathfrak{p}_2$. Thus we have found our CPI and rest the case $r = 2$

$$\mathfrak{p}_0 \;\subset\; \widetilde{\mathfrak{p}}_1 \;\subset\; \mathfrak{p}_2$$

For a general $r \geq 3$ we are given a CPI $(\mathfrak{p}_0, \ldots, \mathfrak{p}_r)$ of R with $a \in \mathfrak{p}_r$. Thus we can use the induction hypothesis on the truncated chain $(\mathfrak{p}_1, \ldots, \mathfrak{p}_r)$ and find $\widetilde{\mathfrak{p}}_k$ where $k \in 2 \ldots r-1$ such that $a \in \widetilde{\mathfrak{p}}_2$. But then we can also look at $(\mathfrak{p}_0, \mathfrak{p}_1, \widetilde{\mathfrak{p}}_2)$. By the case $r = 2$ there is another prime ideal $\widetilde{\mathfrak{p}}_1$ with $a \in \widetilde{\mathfrak{p}}_2$. And thus we have found the chain $(\mathfrak{p}_0, \widetilde{\mathfrak{p}}_1, \ldots, \widetilde{\mathfrak{p}}_{r-1}, \mathfrak{p}_r)$ we required.

(ii) We are now ready to prove (b) $\implies$ (a) in (ii), which we do by induction on n. The case $n = 1$ is (i) precisely, so we have to perform the induction step for $n \geq 2$: Let $(\mathfrak{p}_0, \ldots, \mathfrak{p}_r)$ be a CPI of R with $\mathfrak{p}_r = \mathfrak{p}$. By assumption $\mathfrak{p}$ is minimal over $\mathfrak{a} = \langle a_1, \ldots, a_n \rangle_{\mathfrak{i}}$. As $a_1 \in \mathfrak{p}$ we may use (iii) to find another CPI $(\mathfrak{p}_0, \widetilde{\mathfrak{p}}_1, \ldots, \widetilde{\mathfrak{p}}_{r-1}, \mathfrak{p}_r)$ of the same length, with $a_1 \in \widetilde{\mathfrak{p}}_1$. Thus, without loss of generality, we may take to this chain and suppose $a_1 \in \mathfrak{p}_1$ already. Now let $\mathfrak{a}_1 := a_1 R$ and for any $k \in 2 \ldots n$ we write $\overline{a}_k := a_k + \mathfrak{a}_1 \in R/\mathfrak{a}_1$. By the correspondence theorem of ideals (1.71) we then find a CPI in $R/\mathfrak{a}_1$ given by

$$\mathfrak{p}_1 \big/ \mathfrak{a}_1 \;\subset\; \ldots \;\subset\; \mathfrak{p}_r \big/ \mathfrak{a}_1 \;=\; \mathfrak{p} \big/ \mathfrak{a}_1$$

As this chain is of length $r-1$ we conclude $r - 1 \leq \operatorname{height}(\mathfrak{p}/\mathfrak{a}_1)$. Let us abbreviate $\overline{\mathfrak{a}} := \mathfrak{a}/\mathfrak{a}_1$ and likewise with any over ideal $\mathfrak{p}_k$. Then we claim, that $\overline{\mathfrak{p}} = \mathfrak{p}/\mathfrak{a}_1$ is minimal over $\overline{\mathfrak{a}}$: Suppose there was some prime ideal in between $\overline{\mathfrak{a}} \subseteq \overline{\mathfrak{p}}' \subseteq \overline{\mathfrak{p}}$ then (by the correspondence theorem of ideals again) $\overline{\mathfrak{p}}'$ would be of the form $\overline{\mathfrak{p}}' = \mathfrak{p}'/\mathfrak{a}_1$ for some $\mathfrak{p}' \in \operatorname{Spec}(R)$ with $\mathfrak{a}_1 \subseteq \mathfrak{p}'$. In particular $a_1 \in \mathfrak{p}'$. And as $\overline{a}_k \in \overline{\mathfrak{a}} \subseteq \overline{\mathfrak{p}}'$ we also get $a_k \in \mathfrak{p}'$ for any $k \in 2 \ldots n$. Together this is $a_k \in \mathfrak{p}'$ for any $k \in 1 \ldots n$ and hence $\mathfrak{a} \subseteq \mathfrak{p}'$. As also $\mathfrak{p}' \subseteq \mathfrak{p}$ by assumption, but $\mathfrak{p}$ is minimal over $\mathfrak{a}$, we conclude $\mathfrak{p}' = \mathfrak{p}$ and hence $\overline{\mathfrak{p}}' = \overline{\mathfrak{p}}$. That is $\overline{\mathfrak{p}}$ truly is minimal over $\overline{\mathfrak{a}}$.

But $R/\mathfrak{a}_1$ is a noetherian ring again and $\overline{\mathfrak{a}} = \langle \overline{a}_2, \ldots, \overline{a}_n \rangle_{\mathfrak{i}}$ is generated by $n-1$ elements (clearly $\overline{a}_1 = 0$ does not contribute). Hence we may use the induction hypothesis for $\overline{\mathfrak{p}}$, which yields the estimate $\operatorname{height}(\overline{\mathfrak{p}}) \leq n-1$. Let us combine the inequalities we found

$$r - 1 \;\leq\; \operatorname{height}(\overline{\mathfrak{p}}) \;\leq\; n - 1$$

That is $r \leq n$. And as we started with an arbitrary CPI ending in $\mathfrak{p}$ there are no CPIs in R of length greater n, that end in $\mathfrak{p}$. And this means $\operatorname{height}(\mathfrak{p}) \leq n$ as claimed.

(iii) Pick up a prime ideal $\mathfrak{p} \in \operatorname{Spec}(R)$ that is minimal over $\mathfrak{a}$, which is possible, according to (2.18). As $\mathfrak{a} \subseteq \mathfrak{p}$, we have $\operatorname{height}(\mathfrak{a}) \leq \operatorname{height}(\mathfrak{p})$. Now pick up some $a_k \in R$ such that $\mathfrak{a} = \langle a_1, \ldots, a_n \rangle_{\mathfrak{i}}$ where $n = \operatorname{rank}(\mathfrak{a})$. Then $\mathfrak{p}$ is a prime ideal, that is minimal over $\langle a_1, \ldots, a_n \rangle_{\mathfrak{i}}$ and thereby $\operatorname{height}(\mathfrak{p}) \leq n$ by the (b) $\implies$ (a) part, of (ii). Together this is

$$\operatorname{height}(\mathfrak{a}) \;\leq\; \operatorname{height}(\mathfrak{p}) \;\leq\; n \;=\; \operatorname{rank}(\mathfrak{a})$$

(iv) **Case 1:** For $n = m$ we only have to consider any prime ideal $\mathfrak{p}_m$ minimal over $\mathfrak{a}_m = \mathfrak{a} = \langle a_1, \ldots, a_m \rangle_{\mathfrak{i}}$. By the (b) $\implies$ (a) part in (ii) we also know $\operatorname{height}(\mathfrak{p}_m) \leq m$. But as $\mathfrak{a} \subseteq \mathfrak{p}_m$ we also have $m = \operatorname{height}(\mathfrak{a}) \leq \operatorname{height}(\mathfrak{p}_m)$. Together this is $\operatorname{height}(\mathfrak{p}_m) = m$ for any prime ideal $\mathfrak{p}_m$ of R, that is minimal over $\mathfrak{a}$.

Case 2: For $n = m + 1$ we argue in the following way: Recall that $\mathbb{V}(\mathfrak{a})_*$ denotes the set of prime

ideals, minimal over $\mathfrak{a}$ and *suppose* we had

$$\mathfrak{b} \;\subseteq\; \bigcup \mathbb{V}(\mathfrak{a})_*$$

As R is a noetherian ring, $\mathbb{V}(\mathfrak{a})_*$ is a finite set, according to (2.45.(iv)). So $\mathfrak{b}$ is contained in a finite union of prime ideals and hence by prime avoidance (2.14.(iii)) it is contained $\mathfrak{b} \subseteq \mathfrak{p}$ in one of those $\mathfrak{p} \in \mathbb{V}(\mathfrak{a})_*$. That is $\mathfrak{p}$ would be a prime ideal, that also is minimal over $\mathfrak{a}$. As $\mathfrak{a} = \langle a_1, \ldots, a_m \rangle_{\mathfrak{i}}$ the (b) $\implies$ (a) part of (ii) yields $\operatorname{height}(\mathfrak{p}) \leq m$. But as $\mathfrak{b} \subseteq \mathfrak{p}$ we have

$$m \;<\; n \;\leq\; \operatorname{height}(\mathfrak{b}) \;\leq\; \operatorname{height}(\mathfrak{p}) \;\leq\; m$$

This contradiction shows $\mathfrak{b} \not\subseteq \mathfrak{p}$ for any prime ideal, minimal over $\mathfrak{a}$ and hence (due to prime avoidance) the above inclusion of $\mathfrak{b}$ is *untrue*. That is there is some $a_n \in R$ such that

$$a_n \;\in\; \mathfrak{b} \setminus \bigcup \mathbb{V}(\mathfrak{a})_*$$

It remains to prove, that any prime ideal $\mathfrak{p}_n$ minimal over $\mathfrak{a}_n$ has $\operatorname{height}(\mathfrak{p}_n) = 0$. Note that $\mathfrak{a}_n = a_1R + \cdots + a_nR = \mathfrak{a} + a_nR$ and therefore $\operatorname{height}(\mathfrak{p}_n) \leq n$ by the (b) $\implies$ (a) part of (ii). Conversely, as we have $\mathfrak{a} \subseteq \mathfrak{a}_n \subseteq \mathfrak{p}_n$ there is some prime ideal $\mathfrak{p}'$ of R, that is minimal over $\mathfrak{a}$, by (2.18.(iv)). By construction this means $a_n \notin \mathfrak{p}'$. But as $a_n \in \mathfrak{a}_n \subseteq \mathfrak{p}_n$ we have $a_n \in \mathfrak{p}_n \setminus \mathfrak{p}'$. In particular we have a strict inclusion $\mathfrak{p}' \subset \mathfrak{p}_n$ and thereby $\operatorname{height}(\mathfrak{p}') < \operatorname{height}(\mathfrak{p}_n)$ by (vi). But by case 1 we know $\operatorname{height}(\mathfrak{p}') = m$ such that we conclude $\operatorname{height}(\mathfrak{p}_n) = m+1 = n$ from

$$m \;=\; \operatorname{height}(\mathfrak{p}') \;<\; \operatorname{height}(\mathfrak{p}_n) \;\leq\; n \;=\; m+1$$

Case 3: For $n \geq m+2$ we use induction on $n-m$. We have dealt with $n-m=0$ in case 1 and case 2 was the foundation of the induction, as $n-m=1$. Then we continue and have $\operatorname{height}(\mathfrak{p}_{n-1}) = n-1$ for any prime ideal $\mathfrak{p}_{n-1}$ that is minimal over $\mathfrak{a}_{n-1}$. In particular $\operatorname{height}(\mathfrak{a}_{n-1}) = n-1$ by (8.69.(viii)). Then by case 2 again we conclude, that there is some $a_n \in \mathfrak{b}$ such that $\operatorname{height}(\mathfrak{p}_n) = n$ for any prime ideal $\mathfrak{p}_n$ that is minimal over $\mathfrak{a}_n$. And this had to be proved.

(ii) Now we are ready for (a) $\implies$ (b): Let $r := \operatorname{height}(\mathfrak{p}) \leq n$ and use (iv) with the following parameters: $m = 0$, $n = r$, $\mathfrak{a} = 0$ and $\mathfrak{b} = \mathfrak{p}$. Then there are some $a_1, \ldots, a_r \in \mathfrak{p}$, such that for any prime ideal $\mathfrak{p}'$ of R, that is minimal over $\mathfrak{a}_r = \langle a_1, \ldots, a_r \rangle_{\mathfrak{i}}$ we have $\operatorname{height}(\mathfrak{p}') = r$. By construction we have $\mathfrak{a}_r \subseteq \mathfrak{p}$, now suppose $\mathfrak{p}$ was not minimal over $\mathfrak{a}_r$. Then there would be some prime ideal $\mathfrak{p}'$ with $\mathfrak{a}_r \subseteq \mathfrak{p}' \subseteq \mathfrak{p}$, that is minimal over $\mathfrak{a}_r$. In particular $\operatorname{height}(\mathfrak{p}') = r$. Once again (vi) would turn $\mathfrak{p}' \subseteq \mathfrak{p}$ into $r = \operatorname{height}(\mathfrak{p}') < \operatorname{height}(\mathfrak{p}) = r$, from which we conclude $\mathfrak{p}' = \mathfrak{p}$. That is $\mathfrak{p}$ is minimal over $\mathfrak{a}_r$ such that we have found the elements $a_1, \ldots, a_r$. If the n in (ii) exceeds r, just fill up $a_{r+1} = \cdots = a_n = 0 \in \mathfrak{p}$, then $\langle a_1, \ldots, a_n \rangle_{\mathfrak{i}} = \mathfrak{a}_r$ is unchanged and hence $\mathfrak{p}$ is minimal over $\langle a_1, \ldots, a_n \rangle_{\mathfrak{i}}$ too.

(vi) Clearly we use induction on r: For $r = 0$ we have $\mathfrak{a}_0 = 0$ such that $\operatorname{height}(\mathfrak{a}_0) = 0$ is granted. Also, as we started with a CPI $\mathfrak{p}_0$ is a minimal ideal and hence $\mathfrak{p}_0$ is minimal over $\mathfrak{a}_0$.

For the induction step, we use (v) with the following parameters: $m = r-1$, $n = r$, $\mathfrak{a} := \mathfrak{a}_{r-1}$ and $\mathfrak{b} := \mathfrak{p}_r$. Then by (v) there is some $a_r \in \mathfrak{p}_r$ such that for any prime ideal $\mathfrak{p}'$ minimal over $\mathfrak{a}_r$ he

have height$(\mathfrak{p}') = r$. In particular we already have height$(\mathfrak{a}_r) = r$. And as $\mathfrak{a}_{r-1} \subseteq \mathfrak{p}_{r-1} \subseteq \mathfrak{p}_r$ and $a_r \in \mathfrak{p}_r$ we have $\mathfrak{a}_r \subseteq \mathfrak{p}_r$ by construction. It remains to prove, that $\mathfrak{p}_r$ is minimal over $\mathfrak{a}_r$. So suppose it was not, then there was some $\mathfrak{p}'$ with $\mathfrak{a}_r \subseteq \mathfrak{p}' \subset \mathfrak{p}_r$. In particular height$(\mathfrak{p}') <$ height$(\mathfrak{p}_r)$. As $\mathfrak{a}_r \subseteq \mathfrak{p}'$ we have $r =$ height$(\mathfrak{a}_r) \leq$ height$(\mathfrak{p}') <$ height$(\mathfrak{p}_r) = r$. From this contradiction, we find that there is no such $\mathfrak{p}'$ and hence $\mathfrak{p}_r$ is minimal over $\mathfrak{a}_r$, as claimed.

(vii) Suppose we had height$(\mathfrak{p}) = 0$, then $\mathfrak{p}$ would be a minimal prime and as such $\mathfrak{p} \subseteq \text{ZD}(R)$, by (2.19.(ii)). But as $a \in \text{NZD}(R)$ and $a \in \mathfrak{p}$ this is untrue, such that height$(\mathfrak{p}) \geq 1$. Also, as R is a noetherian ring, $\mathfrak{p}$ is of finite height, by (ii), such that (8.69.(xii)) already tells us height$(\mathfrak{p}/aR) <$ height$(\mathfrak{p})$. In other words that is the inequality

$$\text{height}\left(\mathfrak{p}\,\middle/_{aR}\right) \;\leq\; \text{height}(\mathfrak{p}) - 1$$

Also, as $\mathfrak{p}$ is of finite height, we may pick up a CPI $(\mathfrak{p}_0, \ldots, \mathfrak{p}_r)$ in R such that $\mathfrak{p}_r = \mathfrak{p}$ and $r =$ height$(\mathfrak{p})$. And as we also have (iv) there is another CPI $(\mathfrak{p}_0, \widetilde{\mathfrak{p}}_1, \ldots, \widetilde{\mathfrak{p}}_{r-1}, \mathfrak{p}_r)$ such that $a \in \widetilde{\mathfrak{p}}_1$. Then we find a CPI in R/aR of length $r-1$

$$\widetilde{\mathfrak{p}}_1\,\big/_{aR} \;\subset\; \ldots \;\subset\; \widetilde{\mathfrak{p}}_{r-1}\,\big/_{aR} \;\subset\; \mathfrak{p}\,\big/_{aR}$$

ending in $\mathfrak{p}/aR$. In particular height$(\mathfrak{p}/aR) \geq r - 1 =$ height$(\mathfrak{p}) - 1$. Thus we have found the converse inequality, too and hence the equality of the two terms.

□

Proof of (8.82):

(2) As xz and $yz \in zR$ we have $\mathfrak{a} \subseteq zR$. And as $\mathfrak{a} \subseteq zR \subset yR + zR \subset xR + yR + zR$ is a CPI in R the correspondence theorem tells us, that $\overline{z}A \subset \overline{y}A + \overline{z} \subset \overline{x}A + \overline{y}A + \overline{z}A$ is a CPI of A. In particular we have kdim$(A) \geq 2$. Conversely suppose we had kdim$(A) \geq 3$, then there was some CPI $(\mathfrak{q}_0, \ldots, \mathfrak{q}_3)$ of length 3 inside A and therefore height$(\mathfrak{q}_3) \geq 3$. But by the correspondence theorem $\mathfrak{q}_3$ is of the form $\mathfrak{q}_3 = \mathfrak{p}_3/\mathfrak{a}$ for some $\mathfrak{p}_3 \in \text{Spec}(R)$. In particular we have height$(\mathfrak{p}_3) \leq 3$ and as $xz \in \mathfrak{a}$ is a non-zero-divisor we have $3 \leq$ height$(\mathfrak{q}_3) \leq$ height$(\mathfrak{p}_3) - 1 \leq 2$. From this contradiction we get kdim$(A) \leq 2$ and hence kdim$(A) = 2$.

(1) For (1) suppose $\mathfrak{a} \subseteq \mathfrak{p} \subseteq zR$, then $xz \in \mathfrak{p}$ such that $x \in \mathfrak{p}$ or $z \in \mathfrak{p}$. As $x \in zR$ is untrue, we find $z \in \mathfrak{p}$ and thereby $zR \subseteq \mathfrak{p}$ which turns into $\mathfrak{p} = zR$. Thus zR is a minimal prime over $\mathfrak{a}$. Likewise $\mathfrak{a} \subseteq \mathfrak{p} \subseteq xR + yR$ yields xz and $yz \in \mathfrak{p}$ such that $\{x, y\} \subseteq \mathfrak{p}$ or $z \in \mathfrak{p}$. Again $z \in xR + yR$ is untrue such that we have $xR + yR \subseteq \mathfrak{p}$ from which we have $\mathfrak{p} = xR + yR$. Thus $xR + yR$ also is a prime ideal, minimal over $\mathfrak{a}$.

(3) It remains to prove (3): To do this consider any $f \in R = E[x, y, z]$. We split this polynomial into three separate parts

$$\begin{aligned} f &= \sum_{i=0}^{\infty}\sum_{j=0}^{\infty}\sum_{k=0}^{\infty} f[i,j,k]x^i y^j z^k \\ &= \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} f[i,j,0]x^i y^j + \sum_{k=1}^{\infty} f[i,j,k]x^i y^j z^k \end{aligned}$$

$$= \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} f[i,j,0]x^iy^j + \sum_{k=1}^{\infty}\left(f[0,0,k]z^k + \sum_{(i,j)\neq(0,0)} f[i,j,k]x^iy^jz^k \right)$$

Hereby $f(\overline{x},\overline{y},\overline{z}) = f + \mathfrak{a}$ and for any $(i,j) \neq 0$ and $k \geq 1$ we have $x^iy^jz^k + \mathfrak{a} = 0 + \mathfrak{a}$, as both xz and $yz \in \mathfrak{a}$. Thus the residue class of f only retains the terms

$$f(\overline{x},\overline{y},\overline{z}) \;=\; \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} f[i,j,0]\overline{x}^i\overline{y}^j + \sum_{k=1}^{\infty} f[0,0,k]\overline{z}^k$$

Note that this is a basis representation of $\overline{f}$ in the remaining basis of A. In particular if $g \in E[t_1,t_2]$ then $g(\overline{x},\overline{y}) = 0$ implies $g[i,j] = 0$ for and i, $j \in \mathbb{N}$ and therefore $g = 0$. Thus $\overline{x}$ and $\overline{y}$ are algebraically independent. Yet $\overline{z}$ is algebraic over $P := E[\overline{x},\overline{y}]$, as it satisfies the polynomial $\overline{x}t \in P[t]$. As P is an integral domain $P[\overline{z}] : P$ is an algebraic extension, but $P[\overline{z}] = A$ is clear.

(4) By (1) $\overline{\mathfrak{q}} = \langle x,y\rangle_{\mathfrak{i}}/\mathfrak{a} = \overline{x}A + \overline{y}A$ is minimal over $\mathfrak{a}$ such that $\mathrm{height}(\overline{\mathfrak{q}}) = 0$. And in (2) we have found a CPI of length 2 ending in $\overline{\mathfrak{m}} = \langle x,y,z\rangle_{\mathfrak{i}}/\mathfrak{a} = \overline{x}A + \overline{y}A + \overline{x}A$, such that $2 \leq \mathrm{height}(\overline{\mathfrak{m}}) \leq \mathrm{kdim}(A) = 2$. Now for $\overline{\mathfrak{m}}/\overline{\mathfrak{q}}$: If there was some prime ideal in between, by the correspondence theorem, this could have to be of the form $\mathfrak{p}'/\mathfrak{a}$ for some $xR + yR \subset \mathfrak{p}' \subset xR + yR + zR$. But in $R = E[x,y,z]$ it is known from (8.77.(ii)) that $\mathrm{height}(xR + yR + zR) = \mathrm{height}(xR + yR) + 1$. Thus there is no room for such a $\mathfrak{p}'$ and therefore $\mathrm{height}(\overline{\mathfrak{m}}/\overline{\mathfrak{q}}) = 1$, too.

□

Proof of (8.83): (■)

Nota The proof of this example is a little sketchy and we will not prove all the statements of the claim - only enough to complete the counter-example. We feel, that this suffices, as this is an example, not a theorem. It warrants the black-box brand however.

Let us abbreviate $A := E[x,y,z]$. As $E[t]$ is an integral domain, so is the image $\mathrm{im}(\pi) \;\leq_{\mathrm{r}}\; E[t]$ and this implies, that $\mathfrak{p} = \mathrm{kn}(\pi)$ is a prime ideal. Also $\pi(f)(0) = f(0,0,0)$ such that $f \in \mathfrak{p}$ [and hence $\pi(f) = 0$] implies $f \in \mathfrak{m}$. Therefore $\mathfrak{p} \subseteq \mathfrak{m}$, but as $x \in \mathfrak{m}$ yet $x \notin \mathfrak{p}$ we have $\mathfrak{p} \subset \mathfrak{m}$. As E is a field, we have $\mathrm{kdim}(A) = 3$, according to (8.77.(i)) or (8.85.(v)). And as $\mathfrak{p} \subset \mathfrak{m}$ we conclude $\mathrm{height}(\mathfrak{p}) \leq 2$. In fact $\mathrm{height}(\mathfrak{p}) = 2$, but we do not prove this here (■) . Time to introduce the next abbreviation: For $\alpha = (\alpha_1,\alpha_2,\alpha_3) \in \mathbb{N}^3$ let us denote $\omega(\alpha) := 3\alpha_1 + 4\alpha_2 + 5\alpha_3$. Then for any $f \in A$ it is clear, that

$$\pi(f) \;=\; f(t^3,t^4,t^5) \;=\; \sum_{\alpha\in\mathbb{N}^3} f[\alpha]\, t^{\omega(\alpha)} \;=\; \sum_{k=0}^{\infty}\left(\sum_{\omega(\alpha)=k} f[\alpha] \right) t^k$$

Let $A_k := \pi^{-1}(Et^k) = \mathrm{Lh}\{\, x^{\alpha_1}y^{\alpha_2}z^{\alpha_3} \mid \omega(\alpha) = k \,\}$ be A_k is the k-homogeneous component of A under the grading $\deg_\omega$. Consider any $f \in A$ and let $f = \sum_k f_k$ where $f_k \in A_k$. This is the decomposition of f into ω-homogeneous components. Then we can write the identity above, in the following form

$$\pi(f) \;=\; \sum_{k=0}^{\infty}\left(\sum_{\omega(\alpha)=k} f[\alpha] \right) t^k \;=\; \sum_{k=0}^{\infty} f_k(1,1,1)\, t^k$$

Thus we have $f \in \mathfrak{p}$ if and only if $\sum_{\omega(\alpha)=k} f[\alpha] = 0$ for any $k \in \mathbb{N}$. In other words, that is $f \in \mathfrak{p}$ is equivalent to $f_k(1,1,1) = 0$ for any $k \in \mathbb{N}$. In particular, if for some $k \in \mathbb{N}$ there is only one $\alpha \in \mathbb{N}^3$

satisfying $\omega(\alpha) = k$, then $f \in \mathfrak{p}$ implies $f[\alpha] = 0$. Let us compile a table of all the monomials in A of ω-degree up to 10:

monomials	ω
$\mathbf{1}$	0
x	3
y	4
z	5
x^2	6
xy	7
xz, y^2	8
yz, x^3	9
x^2y, z^2	10

By checking a list of all $\alpha \in \mathbb{N}^3$ of absolute value $|\alpha| \leq 3$ we see that any other monomial has an ω-degree exceeding 10. And from our table we find, that $\mathfrak{p}$ does not contain any element $f \in A$ of $\deg_\omega(f) \leq 7$. It does contain $f_1 = xz - y^2$, $f_2 = yz - x^3$ and $x^2y - z^2$ however. Note that these are homogeneous polynomials $f_1 \in A_8$, $f_2 \in A_9$ and $f_3 \in A_{10}$. In particular we have $\langle f_1, f_2, f_3 \rangle_i \subseteq \mathfrak{p}$. In fact these ideals even are equal, but we do not prove this here (■) . We settle with pointing out, that

$$\begin{aligned} x^4 - y^3 &= y(xz - y^2) - x(yz - x^3) \\ x^5 - z^3 &= z(x^2 - z^2) - x^2(yz - x^3) \\ y^5 - z^4 &= (x^2y + z^2)(x^2y - z^2) - y^2(x^4 - y^3) \end{aligned}$$

Let us now assume, that $\mathfrak{p}$ was generated by 2 elements $\{ p_1, p_2 \} \subseteq A$. That if we regard $\mathfrak{p}$ as an A-module we have a surjective homomorphism of A-modules

$$A^2 \twoheadrightarrow \mathfrak{p} \,:\, (f_1, f_2) \mapsto f_1 p_1 + f_2 p_2$$

So what happens if we tensor this homomorphism with $A/\mathfrak{m}$ from the right? By (3.146.(ii)) we have an isomorpism of A-modules of the form

$$\mathfrak{p} \otimes {}^{A}\!\Big/_{\mathfrak{m}} \xrightarrow{\sim} {}^{\mathfrak{p}}\!\Big/_{\mathfrak{m}\mathfrak{p}} \,:\, p \otimes (a + \mathfrak{m}) \mapsto ap + \mathfrak{m}\mathfrak{p}$$

Note that $E \xrightarrow{\sim} A/\mathfrak{m} : a \mapsto a + \mathfrak{m}$ is a canonical isomorphism, by construction of $\mathfrak{m}$. Also A^2 is a free A-module, having the basis elements $(1,0)$ and $(0,1)$. Therefore by (3.146.(v)) we find another isomorphism of A-modules, this time

$$E^2 \xrightarrow{\sim} \left({}^{A}\!\Big/_{\mathfrak{m}}\right)^2 \xrightarrow{\sim} A^2 \otimes {}^{A}\!\Big/_{\mathfrak{m}} \,:\, (a,b) \mapsto \begin{pmatrix}1\\0\end{pmatrix} \otimes (a + \mathfrak{m}) + \begin{pmatrix}0\\1\end{pmatrix} \otimes (b + \mathfrak{m})$$

Note that the image of (a,b) under this isomorphism can be written in the form $(a,b) \otimes (1 + \mathfrak{m})$. This is the form we in the next step. As tensoring is right-exact (3.156) it preserves the surjectivity of the homomorphism above, that is we get a surjective homomorphism of the following form

$$A^2 \otimes {}^{A}\!\Big/_{\mathfrak{m}} \twoheadrightarrow \mathfrak{p} \otimes {}^{A}\!\Big/_{\mathfrak{m}} \,:\, (f_1, f_2) \otimes (a + \mathfrak{m}) \mapsto (f_1 p_1 + f_2 p_2) \otimes (a + \mathfrak{m})$$

Note that $(a,b)\otimes(1+\mathfrak{m})$ is mapped to $(ap_1+bp_2)\otimes(1+\mathfrak{m})$ under this epimorphism. Let us now insert both of the isomorphisms we have found above, then this epimorphism turns into the following epimorphism (of A-modules still).

$$E^2 \twoheadrightarrow \mathfrak{p}\Big/_{\mathfrak{m}\mathfrak{p}} : (a,b) \mapsto ap_1+bp_2+\mathfrak{m}\mathfrak{p}$$

That is we would have $\mathfrak{p}=Ep_1+Ep_2+\mathfrak{m}\mathfrak{p}$. But $\mathfrak{m}\mathfrak{p}$ contains elements of ω-degree no less than 11 (at least 3 from x and 8 from any element of $\mathfrak{p}$. Thus for any $f\in\mathfrak{p}$ the coefficients of f and ap_1+bp_2 of ω-degree up to 10 have to agree. In particular this is true for f_1, f_2 and f_3 as these are of ω-degree up to 10. Let $\overline{p}_i$ be the first 10 ω-coefficients of p_i, then we have argued, that

$$\{\, f_1,f_2,f_3 \,\} \quad\subseteq\quad \mathrm{Lh}_E\{\, \overline{p}_1,\overline{p}_2 \,\}$$

But $\{\, f_1,f_2,f_3 \,\}$ is E-linearly independent, so this set cannot be contained in a space of dimension 2 (or less). And this means that $\mathfrak{p}$ cannot have less than 3 generators. □

Nota This example is given as *exercise* 1.11 in the very first chapter in Hartshorne (GTM 52). And note that we did not even give a full prove here. We leave it to the reader to decide whether Hartshorne (a) saw an easy way to do it, that we don't (b) was careless not to check, whether it can be done easily or (c) just didn't mind to demotivate his readers. It is precisely the existence of such exercises that drove this book's author to write this text, as he frowns upon people of the (b) and (c)-kinds.

Proof of (8.85):

(i) The implication (a) $\implies$ (b) is easy: For $\mathfrak{u}=\mathfrak{p}[t]$ we may take $\mathfrak{v}:=\mathfrak{p}[t]+tR[t]$ which is given to be $\mathfrak{v}=\{\, p+tf \mid p\in\mathfrak{p}, f\in R[t]\,\}$. Then $\mathfrak{v}\cap R=\mathfrak{p}=\mathfrak{u}\cap R$ is clear by construction. Also we have $t\in\mathfrak{v}$ but $t\notin\mathfrak{u}=\mathfrak{p}[t]$, as this would mean $1\in\mathfrak{p}$. And finally we know that $R[t]/\mathfrak{v}$ and $R/\mathfrak{p}$ are isomorphic, according to (3.43.(iv)). As $R/\mathfrak{p}$ is an integral domain ($\mathfrak{p}$ is prime), so is $R[t]/\mathfrak{v}$ and this means that $\mathfrak{v}$ is a prime ideal again. Altogether, we have (b).

Conversely for (b) $\implies$ (a) we first note that $\mathfrak{p}[t]=\mathfrak{p}R[t]=(\mathfrak{u}\cap R)R[t]\subseteq\mathfrak{u}$ is generally true, according to (8.15). We now assume the inclusion was strict $\mathfrak{p}[t]\subset\mathfrak{u}$ and deduce a contradiction - then we have proved $\mathfrak{p}[t]=\mathfrak{u}$. So let us assume $\mathfrak{p}[t]\subset\mathfrak{u}\subset\mathfrak{v}$ was a CPI in $R[t]$, then we obtain another CPI in $R[t]/\mathfrak{p}[t]$ by virtue of

$$0 \;=\; \mathfrak{p}[t]\Big/_{\mathfrak{p}[t]} \;\subset\; \mathfrak{u}\Big/_{\mathfrak{p}[t]} \;\subset\; \mathfrak{v}\Big/_{\mathfrak{p}[t]}$$

Let us abbreviate $\overline{R}:=R/\mathfrak{p}$. For any $a\in R$ let us also abbreviate $\overline{a}:=a+\mathfrak{p}\in\overline{R}$ and for any polynomial $f\in R[t]$ denote $\overline{f}:=\sum_k(f[k]+\mathfrak{p})t^k\in\overline{R}[t]$. Note that there is a canonical isomorphism $R[t]/\mathfrak{p}[t]\xrightarrow{\sim}\overline{R}[t]$, given by $f+\mathfrak{p}[t]\mapsto\overline{f}$, due to (3.43.(iii)). We identify these rings under this isomorphism, that is we use it, without explicitly mentioning it. Now let $\overline{U}:=\overline{R}\setminus\{\overline{0}\}$, that is $\overline{E}:=\mathrm{quot}(\overline{R})=\overline{U}^{-1}\overline{R}$. Under this idenfication the ring extension $\overline{R}[t]:\overline{R}$ turns into a ring-extension $R[t]/\mathfrak{p}[t]:\overline{R}$ under the structural homomorphism $\overline{a}\mapsto a\mathbf{1}+\mathfrak{p}[t]$ and we can consider $\overline{U}\subseteq\overline{R}\subseteq\overline{R}[t]$ as a subset of $R[t]/\mathfrak{p}[t]$ in the form of $\overline{U}=\{\, a\mathbf{1}+\mathfrak{p}[t]\mid a\in R\setminus\mathfrak{p}\,\}$. Then it is

easy to see, that

$$\left(\mathfrak{u}\Big/_{\mathfrak{p}[t]}\right)\cap\overline{R} \;=\; \{\,\overline{a}\mid a\mathbf{1}\in\mathfrak{u}\,\} \;=\; \{\,\overline{a}\mid a\in\mathfrak{u}\cap R\,\} \;=\; {}^{\mathfrak{u}\cap R}\Big/_{\mathfrak{p}} \;=\; \{\,\overline{0}\,\}$$

As $0\in\mathfrak{p}$ we have $0\notin R\setminus\mathfrak{p}$ and thereby $\overline{0}\notin\overline{U}$. That is $\mathfrak{u}/\mathfrak{p}[t]\cap\overline{U}=\emptyset$. Likewise $\mathfrak{v}/\mathfrak{p}[t]=(\mathfrak{v}\cap R)/\mathfrak{p}=\{\overline{0}\}$ by assumption (b) on $\mathfrak{v}$ and hence $\mathfrak{v}/\mathfrak{p}[t]\cap\overline{U}=\emptyset$, as well. By (2.129) we find another CPI in $\overline{U}^{-1}(R[t]\mathfrak{p}[t])$, that is given to be

$$\overline{U}^{-1}\left(\mathfrak{p}[t]\Big/_{\mathfrak{p}[t]}\right) \;\subset\; \overline{U}^{-1}\left(\mathfrak{u}\Big/_{\mathfrak{p}[t]}\right) \;\subset\; \overline{U}^{-1}\left(\mathfrak{v}\Big/_{\mathfrak{p}[t]}\right)$$

However, as $R[t]/\mathfrak{p}[t]\;\xrightarrow{\sim}\;\overline{R}[t]$ is an isomorphism we also get an isomorphism of the rings localized in $\overline{U}$, that is $\overline{U}^{-1}(R[t]/\mathfrak{p}[t])\;\xrightarrow{\sim}\;\overline{U}^{-1}(\overline{R}[t])$ under $(f+\mathfrak{p}[t])/\overline{u}\mapsto\overline{f}/\overline{u}$. And as the localisation commutes with polynomial rings (2.132.(i)), we can continue the isomorphies

$$\overline{U}^{-1}\left(R[t]\Big/_{\mathfrak{p}[t]}\right) \;\cong_{\mathrm{r}}\; \overline{U}^{-1}(\overline{R}[t]) \;\cong_{\mathrm{r}}\; (\overline{U}^{-1}\overline{R})[t] \;=\; \overline{E}[t]$$

Yet $\overline{E}$ is a field and hence $\overline{E}[t]$ is a PID, but not a field. That is we have $\operatorname{kdim}(\overline{E}[t])=1$ and therefore there can not be any CPI of length 2 or more. Thus the above chain cannot exist and this is the contradiction, we needed for $\mathfrak{p}[t]=\mathfrak{u}$.

(ii) Let us start with (b) $\implies$ (a), that is we consider any prime ideal $\mathfrak{p}'\in\operatorname{Spec}(R)$ such that $\mathfrak{a}\subseteq\mathfrak{p}'\subseteq\mathfrak{p}$. In particular we have $\mathfrak{a}[t]\subseteq\mathfrak{p}'[t]\subseteq\mathfrak{p}[t]$, but as $\mathfrak{p}[t]$ is minimal over $\mathfrak{a}[t]$ this implies $\mathfrak{p}'[t]=\mathfrak{p}[t]$. And from this again we get $\mathfrak{p}'=\mathfrak{p}'[t]\cap R=\mathfrak{p}[t]\cap R=\mathfrak{p}$. That is $\mathfrak{p}'=\mathfrak{p}$ which is the minimality of $\mathfrak{p}$ over $\mathfrak{a}$.

Conversely, for (a) $\implies$ (a), we start with a prime ideal $\mathfrak{u}'\in\operatorname{Spec}(R[t])$ such that $\mathfrak{a}[t]\subseteq\mathfrak{u}'\subseteq\mathfrak{p}[t]$ and let $\mathfrak{p}':=\mathfrak{u}'\cap R$. We then get $\mathfrak{a}=\mathfrak{a}[t]\cap R\subseteq\mathfrak{u}'\cap R=\mathfrak{p}'$ and $\mathfrak{p}'=\mathfrak{u}'\cap R\subseteq\mathfrak{p}[t]\cap R=\mathfrak{p}$, that is $\mathfrak{a}\subseteq\mathfrak{p}'\subseteq\mathfrak{p}$. By minimality of $\mathfrak{p}$ over $\mathfrak{a}$ we conclude $\mathfrak{p}'=\mathfrak{p}$, in other words $\mathfrak{u}'\cap R=\mathfrak{p}[t]\cap R$. If $\mathfrak{u}'=\mathfrak{p}[t]$ then we have the minimality of $\mathfrak{p}[t]$ over $\mathfrak{a}[t]$ as desired. Suppose we had $\mathfrak{u}'\subset\mathfrak{p}[t]$ then by (i) we would get $\mathfrak{u}'=\mathfrak{p}'[t]=\mathfrak{p}[t]$ again, a contradiction. So must have had $\mathfrak{u}'=\mathfrak{p}[t]$ from the start, which is the minimality of $\mathfrak{p}[t]$ over $\mathfrak{a}[t]$.

(iii) Let $n:=\operatorname{height}(\mathfrak{p})$, in particular we find a CPI $(\mathfrak{p}_0,\ldots,\mathfrak{p}_n)$ is a CPI in R, with $\mathfrak{p}_n=\mathfrak{p}$. Then this turns into a CPI $(\mathfrak{p}_0,[t]\ldots,\mathfrak{p}_n[t])$ in $R[t]$. And from this chain we see $\operatorname{height}(\mathfrak{p})=n\leq\operatorname{height}(\mathfrak{p}[t])$.

Conversely, as $\operatorname{height}(\mathfrak{p})=n$ Krull's height theorem (8.80.(ii)) tells us that $\mathfrak{p}$ is minimal over an ideal $\mathfrak{a}$ generated by n elements $\mathfrak{a}=a_1R+\cdots+a_nR$. Then it is clear, that $\mathfrak{a}[t]=a_1R[t]+\cdots+a_nR[t]$ by (3.40.(ii)). Now by (ii) $\mathfrak{p}[t]$ is minimal over $\mathfrak{a}[t]$. And therefore by Krull's height theorem again, we get $\operatorname{height}(\mathfrak{p}[t])\leq n=\operatorname{height}(\mathfrak{p})$.

(iv) Let us first prove that $\operatorname{kdim}(R)+1\leq\operatorname{kdim}(R[t])$: If $n=\operatorname{kdim}(R)$, then is suffices to construct a CPI of length $n+1$ in $R[t]$ and this can be done, easily: Let $(\mathfrak{p}_0,\ldots,\mathfrak{p}_n)$ be a CPI in R. Then $(\mathfrak{p}_0[t],\ldots,\mathfrak{p}_n[t])$ is a CPI in $R[t]$. Now define

$$\mathfrak{u}_{n+1} \;:=\; \mathfrak{p}_n[t]+tR[t] \;=\; \{\,p+tf\mid p\in\mathfrak{p}_n,f\in R[t]\,\}$$

As we have argued before, in the first part of (i), $\mathfrak{u}_{n+1}$ is a prime ideal of $R[t]$ and $\mathfrak{p}_n[t]\subset\mathfrak{u}_{n+1}$.

Thus $(\mathfrak{p}_0[t], \ldots, \mathfrak{p}_n[t], \mathfrak{u}_{n+1})$ is a CPI of length $n+1$ in $R[t]$ - just what we needed.

Now for the upper bound: Let $(\mathfrak{u}_0, \ldots, \mathfrak{u}_r)$ be any CPI in $R[t]$ and let $\mathfrak{p}_i := \mathfrak{u}_i \cap R \in \operatorname{Spec}(R)$ for any $i \in 0 \ldots r$. Then we clearly have a chain $\mathfrak{p}_0 \subseteq \ldots \subseteq \mathfrak{p}_r$ of prime ideals in R, but the inclusions need not be strict - at this time. So suppose we had $\mathfrak{p}_0 = \mathfrak{p}_1 = \mathfrak{p}_2$, then we can apply (i) to $\mathfrak{u}_0 \subset \mathfrak{u}_1$ as $\mathfrak{u}_0 \cap R = \mathfrak{u}_1 \cap R$ to find $\mathfrak{u}_0 = \mathfrak{p}_0[t]$. Likewise (i) yielded $\mathfrak{u}_1 = \mathfrak{p}_1[t]$ from $\mathfrak{u}_1 \subset \mathfrak{u}_2$ as $\mathfrak{u}_1 \cap R = \mathfrak{u}_2 \cap R$, too. But then we had

$$\mathfrak{u}_0 \;=\; \mathfrak{p}_0[t] \;=\; \mathfrak{p}_1[t] \;=\; \mathfrak{u}_1$$

which is untrue, as we started with a CPI and hence $\mathfrak{u}_0 \subset \mathfrak{u}_1$. In complete analogy this is true for any three consecutive prime ideals $\mathfrak{p}_i \subseteq \mathfrak{p}_{i+1} \subseteq \mathfrak{p}_{i+2}$. That is there may *never* be three consecutive ideals $\mathfrak{p}_i = \mathfrak{p}_{i+1} = \mathfrak{p}_{i+2}$. In other words: At least every other inclusion has to be strict.

Let us regard the case $n = 0$ exemplarily: Assume there was some CPI in $R[t]$ with $r \geq 2$. In particular $\mathfrak{u}_0 \subset \mathfrak{u}_1 \subset \mathfrak{u}_r$. Then we had $\mathfrak{p}_0 \subseteq \mathfrak{p}_1 \subseteq \mathfrak{p}_2$. As these cannot be identical we either have $\mathfrak{p}_0 \subset \mathfrak{p}_1$ or $\mathfrak{p}_1 \subset \mathfrak{p}_2$ (or both). But this would mean a CPI of length 1 in R, which does not exist, as $\operatorname{kdim}(R) = n = 0$. Thus we have $r \leq 1$ and thereby $\operatorname{kdim}(R[t]) = r \leq 1 = 2n+1$.

Generally let i be the number of equalities in the chain $\mathfrak{p}_0 \subseteq \ldots \subseteq \mathfrak{p}_r$. Likewise let j be the number of strict inclusions $\subset$ in this chain, that is $i + j = r$. As at least every other inclusion has to be strict, we have $i \leq (r+1)/2$ and therefore

$$j \;=\; r - i \;\geq\; r - \frac{r+1}{2} \quad\Longrightarrow\quad 2j \;\leq\; 2r - (r+1) \quad\Longrightarrow\quad 2j+1 \;\geq\; r$$

We may take $r = \operatorname{kdim}(R[t])$ by choosing a CPI of maximal length. The length j of the CPI in R is bounded by $j \leq \operatorname{kdim}(R) = n$, however. Then we have found $r \leq 2j+1 \leq 2n+1$, as well.

(v) It suffices to verify this for the polynomial ring $R[t]$ is one variable, the general statement follows immediately, by induction on the number ov varibles.

Let $n := \operatorname{kdim}(R)$, we already know $n+1 \leq \operatorname{kdim}(R[t])$ from (iv) above. It only remains to prove the converse estimate: So pick up a CPI $(\mathfrak{u}_0, \ldots, \mathfrak{u}_r)$ in $R[t]$ with $r = \operatorname{kdim}(R[t])$ and let $\mathfrak{p}_i := \mathfrak{u}_i \cap R$ for any $i \in 1 \ldots r$. Then it is clear that $\mathfrak{p}_0 \subseteq \ldots \subseteq \mathfrak{p}_r$ is a chain of prime ideals, that is not strictly ascending. In fact if we had $\mathfrak{p}_0 \subset \ldots \subset \mathfrak{p}_r$, then we had $n+1 \leq \operatorname{kdim}(R[t]) = r \leq \operatorname{kdim}(R) = n$. Thus there has to be some $k \in 0 \ldots r-1$ such that $\mathfrak{p}_k = \mathfrak{p}_{k+1}$ such that we may take

$$m \;:=\; \max\{\, k \in 0 \ldots r-1 \mid \mathfrak{p}_k = \mathfrak{p}_{k+1} \,\}$$

In particular we have $\mathfrak{p}_m = \mathfrak{p}_{m+1}$, whereas $\mathfrak{u}_m \subset \mathfrak{u}_{m+1}$. Thus we get $\mathfrak{u}_m = \mathfrak{p}_m[t]$ from (i). But then (iii) tells us

$$m \;\leq\; \operatorname{height}(\mathfrak{u}_m) \;=\; \operatorname{height}(\mathfrak{p}_m)$$

That is there is a CPI $(\mathfrak{q}_0, \ldots, \mathfrak{q}_m)$ in R with $\mathfrak{q}_m = \mathfrak{p}_m$. And as m is maximal, we also have $\mathfrak{p}_m = \mathfrak{p}_{m+1} \subset \mathfrak{p}_{m+2} \subset \ldots \subset \mathfrak{p}_r$. Note that $\mathfrak{q}_m = \mathfrak{p}_m = \mathfrak{p}_{m+1} \subset \mathfrak{p}_{m+2}$, such that altogether we can compose the CPI $(\mathfrak{q}_0, \ldots, \mathfrak{q}_m, \mathfrak{p}_{m+2}, \ldots, \mathfrak{p}_r)$ which is of length $r-1$ in R. That is we have $n = \operatorname{kdim}(R) \geq r-1$ and from this we find the claim $\operatorname{kdim}(R[t]) = r \leq n+1$.

□

Proof of (8.84):

- Let $\{ \mathfrak{p}'_i \mid i \in I \}$ be the set of prime ideals $\mathfrak{p}' \in \operatorname{Spec}(R)$ in between $\mathfrak{p} \subset \mathfrak{p}' \subset \mathfrak{q}$. We have to prove, that either $I = \emptyset$ or I is infinite. We will prove this by contradiction, that is we assume $I = 1 \dots n$ for some $1 \leq n \in \mathbb{N}$ and disprove this assumption.

- Let us first consider the case $\mathfrak{p} = 0$ (in particular R is an integral domain). We first prove that $\mathfrak{q}$ is not contained in the union of the $\mathfrak{p}'_i$. Suppose it was

$$\mathfrak{q} \subseteq \bigcup_{i=1}^{n} \mathfrak{p}'_i$$

 then by prime avoidance (2.14.(iii)) we had $\mathfrak{q} \subseteq \mathfrak{p}'_k$ for some $k \in 1 \dots n$ and thereby $\mathfrak{q} = \mathfrak{p}'_k$. But this contradicts $\mathfrak{p}'_k \subset \mathfrak{q}$. Thus there has to be some $u \in \mathfrak{q}$ that is not contained in any of the $\mathfrak{p}'_i$. We can use this to prove that $\mathfrak{q}$ is a minimal prime ideal over uR: Suppose $uR \subseteq \mathfrak{p}' \subseteq \mathfrak{q}$ for some prime ideal $\mathfrak{p}'$. As $u \notin \mathfrak{p}'_i$ for any $i \in 1 \dots n$, $\mathfrak{p}'$ can not be any of these ideals. But these are all ideals strictly in between 0 and $\mathfrak{q}$. As $\mathfrak{p}'$ is not one of those it must be $\mathfrak{p}' = \mathfrak{q}$. And this is the minimality of $\mathfrak{q} \in \mathbb{V}(uR)_*$. Now by (8.80.(i)) we conclude $\operatorname{height}(\mathfrak{q}) \leq 1$. But as $0 \subset \mathfrak{p}'_1 \subset \mathfrak{q}$ we have $\operatorname{height}(\mathfrak{q}) \geq 2$. This contradiction can only be remedied by $I = \emptyset$ (then there is no $\mathfrak{p}'_1$) or infinite I (then we cannot employ prime avoidance).

- Now for general $\mathfrak{p}$: Consider the quotient ring $R/\mathfrak{p}$. Then the prime ideals strictly in between $0 = \mathfrak{p}/\mathfrak{p}$ and $\mathfrak{q}/\mathfrak{p}$ are $\mathfrak{p}'_i/\mathfrak{p}$, by the correspondence theorem of ideals. And by the above, there either are none or infinitely many.

- Let us now prove, that $\operatorname{kdim}(R) \leq 1$ whenever $\operatorname{Spec}(R)$ is finite: Suppose we had $\operatorname{kdim}(R) \geq 2$, then there would be some prime ideals $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \mathfrak{p}_2$. In particular

$$\mathfrak{p}_1 \in \{ \mathfrak{p}' \in \operatorname{Spec}(R) \mid \mathfrak{p}_0 \subset \mathfrak{p}' \subset \mathfrak{p}_2 \}$$

 That is the set on the right hand side is non-empty. By the above this would mean it is infinite. But this contradicts $\operatorname{Spec}(R)$ being finite and this contradiction only leaves $\operatorname{kdim}(R) \leq 1$. Hereby $\operatorname{kdim}(R) = 0$ means R is a field, as in this case 0 is a maximal ideal.

□

Proof of (2.164):

- Let us first prove (a) $\implies$ (b): That is we know R_u is a field and want to prove $E = R[1/u]$ for exactly that $u \neq 0$. That is we consider any $a/b \in E$ and need to show that $a/b = f(1/u)$ for some polynomial $f \in R[t]$. As $b \in R$ we can consider $b/1 \in R_u$. As $b \neq 0$ we have $b/1 \neq 0/1$ and as R_u is a field, this means $b/1 \in (R_u)^*$. That is we find some $b' \in R$ and $m \in \mathbb{N}$, such that $b/1 \cdot b'/u^m = 1/1$ and this is $bb' = u^m$. From this we get $abb' = au^m$ which is $a/b = ab'/u^m \in E$. In particular we have $a/b \in R[1/u]$ and as this is true for any $a/b \in E$ we conclude $E \subseteq R[1/u] \subseteq E$ and hence the equality.

- Conversely the implicatio (b) $\implies$ (a) follows easily: By the universal property (2.120) the homomorphism $\kappa : R \to E : a \mapsto a/1$ induces $\overline{\kappa} : R_u \to E : a/u^k \mapsto (a/1) \cdot (u^k/1)^{-1} = a/u^k$. This

clearly is injective, $a/u^j = b/u^k$ has the same meaning in R_u and E and it is surjective by assumption $E = R[1/u]$: If $f \in R[t]$ let $d := \deg(f)$, then $f(1/u) = \sum_k f[k]1/u^k = (\sum_k f[k]u^{d-k})/u^d \in R_u$. Thus $\overline{\kappa}$ is an isomorphism of rings and in particular R_u is a field.

- The implication (b) $\implies$ (c) is trivial: $1/u \in E$ is an element of E, so if $E = R[1/u]$, then E even is generated by a single element. Now to (c) $\implies$ (b): By assumption we have $E = R[x_1, \ldots, x_n]$ for some $x_i \in E$. Say $x_i = a_i/b_i$ for some a_i, $b_i \in R$ with $b_i \neq 0$. Then we take $u := b_1 \ldots b_n$, which is non-zero, as none of the b_i is. For this u we claim $E = R[1/u]$. Regard any $a/b \in E$, by assumption we have $a/b = f(x_1, \ldots, x_n)$ for some polynomial $f \in R[t_1, \ldots, t_n]$. Now let $m := \max\{\, \alpha_k \mid k \in 1 \ldots n, f[\alpha] \neq 0 \,\}$. Then we compute

$$\frac{a}{b} \;=\; f\left(\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n}\right) \;=\; \sum_{\alpha \in \mathbb{N}^n} f[\alpha]\, \frac{a^\alpha}{b^\alpha} \;=\; \frac{1}{u^{nm}} \sum_{\alpha \in \mathbb{N}^n} f[\alpha]\, a^\alpha \prod_{i=1}^{n} b_i^{m-\alpha_i}$$

 And as the sum right of $1/u^{nm}$ is an element of R, the latter expression is an element of $R[1/u]$ considered as a subset of E. Thus we have $E \subseteq R[1/u] \subseteq E$ again and thereby (b).

□

Proof of (2.167):

(i) As $S \subseteq E$ and E is a field, S is an integral domain. Consider any $f/g \in \mathrm{QUOT}(S)$, that is $f = a/b$ and $g = c/d$ for some a, b, c and $d \in R$ with b, c, $d \neq 0$. Then $f/g = ad/bc \in E$ again, such that $\mathrm{QUOT}(S) = E$ again (to be precise they are canonically isomorphic, but the difference is purely set-theoretic). By assumption $E = R[1/u]$ for some $u \neq 0$. But then $\mathrm{QUOT}(S) = E = R[1/u] \subseteq S[1/u] \subseteq \mathrm{QUOT}(S)$ implies $\mathrm{QUOT}(S) = S[1/u]$ again, such that S is a Goldman domain, as well.

(ii) Let $U := \{\, u^n \mid n \in \mathbb{N} \,\}$. As $u \notin \mathrm{NIL}(R)$ we have $0 \notin U$ and thereby $R_u = U^{-1}R \neq 0$ is not the zero-ring. By (2.18.(v)) we may choose a maximal element of $\{\, \mathfrak{b} \trianglelefteq_{\mathrm{i}} R \mid \mathfrak{b} \subseteq R \setminus U \,\}$. Let $\mathfrak{g}$ be such a maximal element, which is a prime ideal. By the correspondence theorem (2.129) $\mathfrak{g}$ corresponds to a maximal ideal $\mathfrak{g}_u = U^{-1}\mathfrak{g}$ of R_u. Now by (2.132.(ii)) we have the isomorphism

$$\Big(R \Big/ \mathfrak{g}\Big)_{u+\mathfrak{g}} \;\xrightarrow{\sim}\; R_u \Big/ \mathfrak{g}_u \;:\; \frac{a+\mathfrak{g}}{(u+\mathfrak{g})^n} \;\mapsto\; \frac{a}{u^n} + \mathfrak{g}_u$$

 As $\mathfrak{g}_u$ is a maximal ideal of R_u, the quotient $R_u/\mathfrak{g}_u$ is a field, and hence $(R/\mathfrak{g})_{u+\mathfrak{g}}$ is a field, as well. But this is one of the defining properties of a Goldman domain.

(iii) Suppose the polynomial ring $R[t]$ *was* a Goldman domain. As $R[t] \subseteq E[t] \subseteq E(t) = \mathrm{QUOT}(R[t])$ we find that $E[t]$ is an itermediate ring of $E(t) : R[t]$. But by (i) this implies, that $E[t]$ is a Goldman domain, as well. Then $E[t]$ would be a noetherian Goldman domain and therefore had finitely many prime ideals only, by (2.169). But as E is a field, $E[t]$ even has infinitely many maximal ideals, by (2.80) - a contradiction. Thus we have to drop the assumption of $R[t]$ being a Goldman domain.

 Now for the second part: Let $S : R$ be a ring extension and $x \in S$ such that $R[x]$ is a Goldman domain. Then we regard the evaluation epimorphism $\varepsilon : R[t] \twoheadrightarrow R[x] : f \mapsto f(x)$. If this was injective, then it would even be an isomorphism $\varepsilon : R[t] \xrightarrow{\sim} R[x]$. But as $R[x]$ was assumed to be a Goldman domain and $R[t]$ can't be. Thus there can be no isomorphism between $R[t]$ and $R[x]$ and this means ε is not injective. That is there is some $f \in \mathrm{kn}(\varepsilon)$ with $f \neq 0$, in other words f

is an algebraic relation $f(x) = 0$. And as x is algebraic over R, we have $x \in \mathrm{alg}(S : R)$. But by (8.41) the algebraic closure is an R-sub-algebra of S and thereby $R[x] \subseteq \mathrm{alg}(S : R)$. Thus any $y \in R[x]$ is algebraic over R.

(iv) As the equivalence of (a) and (b) has been proved in (2.164.(i)), we start with (b) $\implies$ (c): That is we consider any non-zero prime ideal $\mathfrak{p} \trianglelefteq_{\mathfrak{i}} R$ and need to show $u \in \mathfrak{p}$. Suppose we had $u \notin \mathfrak{p}$, then $\mathfrak{p}$ would correspond to a prime ideal of R_u. But as R_u is a field, the only (prime) ideal of R_u is 0 and this corresponds to $0 \trianglelefteq_{\mathfrak{i}} R$, not to $\mathfrak{p}$. Thus $u \in \mathfrak{p}$. Now to (c) $\implies$ (d): Suppose there was some non-zero ideal $\mathfrak{a} \trianglelefteq_{\mathfrak{i}} R$ such that $u \notin \sqrt{\mathfrak{a}}$. That is $u^n \notin \mathfrak{a}$ for any $n \in \mathbb{N}$ and thereby $\mathfrak{a} \subseteq R \setminus U$ where $U := \{\, u^n \mid n \in \mathbb{N} \,\}$. Thus by (2.18.(v)) there was a maximal element $\mathfrak{p}$ of $\{\, \mathfrak{b} \trianglelefteq_{\mathfrak{i}} R \mid \mathfrak{a} \subseteq \mathfrak{b} \subseteq R \setminus U \,\}$ and this is a prime ideal. Thereby $\mathfrak{p} \neq 0$, as $0 \neq \mathfrak{a} \subseteq \mathfrak{p}$. Thus we have $u \in \mathfrak{p}$ by (c) in contradiction to $\mathfrak{p} \subseteq R \setminus U$. Let us return (d) $\implies$ (a): Consider any $a/b \in E$, as $b \neq 0$ we have $bR \neq 0$ and by (d) therefore $u \in \sqrt{bR}$. That is $u^n \in bR$ for some $n \in \mathbb{N}$, which means $u^n = br$ for some $r \in R$. As $u \neq 0$ we also have $r \neq 0$ and thereby $a/b = ar/br = ar/u^n \in R[1/n]$. As this is true for any $a/b \in E$ we get $E \subseteq R[1/u] \subseteq E$.

(v) If $\mathfrak{g}$ is a Goldman ideal with $\mathfrak{a}$, then $\sqrt{\mathfrak{a}} \subseteq \mathfrak{g}$, as $\mathfrak{g}$ is a prime ideal. From this we get the inclusion from left to right. Conversely suppose there was some u contained in the intersection of the Goldman ideals $\mathfrak{g}$, but not in $\sqrt{\mathfrak{a}}$. That is $u^n \notin \mathfrak{a}$ for any $n \in \mathbb{N}$ and therefore $u + \mathfrak{a} \notin \mathrm{NIL}(R/\mathfrak{a})$. Thus by (ii) there is a Goldman ideal $\overline{\mathfrak{g}}$ of $\overline{R} := R/\mathfrak{a}$ with $\overline{u} := u + \mathfrak{a} \notin \overline{\mathfrak{g}}$ such that $(\overline{R}/\overline{\mathfrak{g}})_{\overline{u}+\overline{\mathfrak{g}}}$ is a field. By the correspondence theorem $\overline{\mathfrak{g}}$ is of the form $\overline{\mathfrak{g}} = \mathfrak{g}/\mathfrak{a}$ for some prime ideal $\mathfrak{g} \trianglelefteq_{\mathfrak{i}} R$, with $\mathfrak{a} \subseteq \mathfrak{g}$. We also have $u \notin \mathfrak{g}$, as $u + \mathfrak{a} \notin \mathfrak{g}/\mathfrak{a}$. Now, by the third isomorphism theorem, we have an isomorphism of the form

$$R \Big/ \mathfrak{g} \xrightarrow{\sim} \overline{R} \Big/ \overline{\mathfrak{g}} \;:\; b + \mathfrak{g} \mapsto (b + \mathfrak{a}) + \overline{\mathfrak{g}}$$

And by (2.119) this induces the following isomorphism of

$$\left(R \Big/ \mathfrak{g}\right)_{u+\mathfrak{g}} \xrightarrow{\sim} \left(\overline{R} \Big/ \overline{\mathfrak{g}}\right)_{\overline{u}+\overline{\mathfrak{g}}} \;:\; \frac{b + \mathfrak{g}}{(u + \mathfrak{g})^n} \mapsto \frac{(b + \mathfrak{a}) + \overline{\mathfrak{g}}}{(\overline{u} + \overline{\mathfrak{g}})^n}$$

By the Goldman ideal $\overline{\mathfrak{g}}$ the ring on the image-side of this isomorphism is a field and hence the ring on the pre-image side is, as well. But this means $R/\mathfrak{g}$ is a Goldman domain and hence $\mathfrak{g}$ is a Goldman ideal of R.

(vi) Let $E := \mathrm{QUOT}(R)$ and $F := \mathrm{QUOT}(S)$ be the respective quotient fields of R and S. If R is a Goldman domain, then there is some $u \in R$ with $u \neq 0$ such that $E = R[1/u]$. We can regard $S[1/u] : R[1/u]$ as a ring extension again, under the scalar multiplication

$$\frac{a}{u^m}\frac{s}{u^n} \;:=\; \frac{as}{u^m u^n}$$

where $a \in R$, $s \in S$ and $m, n \in \mathbb{N}$. Consider any $s/u^n \in S[1/u]$, as $S : R$ is algebraic there is a polynomial $f \in R[t]$ such that $f(s) = 0$. Now take to the polynomial

$$g(t) \;:=\; \sum_{k=0}^{\infty} f[k] u^{kn} t^k \;\in\; R[t]$$

then it is clear that $g(s/u^n) = f(s)/1 = 0$. As this is true for any $s/u^n \in S[1/u]$ we see, that $S[1/u] : R[1/u]$ is algebraic. Yet $R[1/u] = E$ is a field and hence $S[1/u] : E$ is integral, where E is a field. Then by (8.30.(viii)) we conclude that $S[1/u]$ is a field as well and thereby $F = S[1/u]$. But this means S is a Goldman domain, too.

Conversely if S is a Goldman domain, then $F = S[1/v]$ for some $v \in S$ with $v \neq 0$. As F trivially is algebraic over S and S is algebraic over R, by assumption (8.41.(iv)) tells us, that $F : R$ is algebraic, too. As S also if finitely generated, there are some $x_1, \ldots, x_n \in S$, such that $S = R[x_1, \ldots, x_n]$. Then $F = S[1/v] = R[x_1, \ldots, x_n, 1/v]$. As F is algebraic over R there are polynomials $f_i \in R[t]$ such that $f_i(x_i) = 0$ for any $i \in 1 \ldots n$. Likewise there is some $g \in R[t]$ with $g(1/v) = 0$. Let $a_i \in R$ be the leading coefficient of f_i and $b \in R$ be the leading coefficient of g. Then let

$$R_1 \;:=\; R\left[\frac{1}{a_1}, \ldots, \frac{1}{a_n}, \frac{1}{b}\right] \;\subseteq\; E$$

Then $(1/a_i)f_i \in R_1[t]$ is a monic polynomial over R_1 that satisfies $(1/a_i)f_i(x_i) = 0$. Likewise $(1/b)g \in R_1[t]$ satisfies $g(1/v) = 0$. That is F is generated by elements that are integral over R_1 and hence $F : R_1$ is integral. As $R_1 \subseteq E$ and E is a field F is torsion free, as an R_1-module. Thus by (8.30.(viii)) R_1 is a field. Now $R \subseteq R_1 \subseteq E = \mathrm{quot}(R)$ implies $R_1 = E$. That is E is finitely generated, as an R-algebra and hence R is a Goldman domain.

□

Proof of (2.169):

- First assume that R is a (not necessarily noetherian) integral domain such that $\mathrm{Spec}(R)$ is finite. Let $\mathfrak{p}_i$ (where $i \in 1 \ldots n$) be the collection of non-zero prime ideals of R. For any $i \in 1 \ldots n$ we may choose some $u_i \in \mathfrak{p}_i$ with u_i. Then $u := u_1 \ldots u_n \neq 0$, as well, as R is an integral domain. And thereby we have

$$u \;\in\; \bigcap \{\, \mathfrak{p}_1, \ldots, \mathfrak{p}_n \,\} \;=\; \bigcap \{\, \mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \neq 0 \,\}$$

 Thus by (2.167.(iii)) we find that R_u is a field and thereby R is a Goldman domain, by definition.

- Conversely suppose R is a noetherian Goldberg domain, then we are going to prove that $\mathrm{Spec}(R)$ is finite. Well, if R is a field, then $\mathrm{Spec}(R) = \{0\}$ and this is a finite set. So we only need to deal with the case where R is not a field. If $E := \mathrm{quot}(R)$, then by assumption we have $E = R[1/u]$ for some $u \neq 0$. By (2.167.(iii)) this means, that $u \in \mathfrak{p}$ for any $\mathfrak{p} \in \mathrm{Spec}(R)$ with $\mathfrak{p} \neq 0$. Let $\mathfrak{a} := uR$ be the ideal generated by u. If we had $\mathfrak{a} = R$, then $1 = uv$ for some $v \in R$ and hence $u \in R^*$. Thus we had $E = R[1/u] = R$, which is R is a field. This has already been dealt with. So we continue with $\mathfrak{a} \neq R$. By (2.45.(iv)) there are finitely many prime ideals, minimal over $\mathfrak{a}$

$$\mathbb{V}(\mathfrak{a})_* \;=\; \{\, \mathfrak{p}_1, \ldots, \mathfrak{p}_m \,\}$$

 So by Krull's principal ideal theorem (8.80.(i)) we get $\mathrm{height}(\mathfrak{p}_i) \leq 1$ for any $i \in 1 \ldots m$. And as $0 \neq u_i \in \mathfrak{p}_i$ we have $0 \subset \mathfrak{p}_i$ such that even $\mathrm{height}(\mathfrak{p}_i) = 1$.

- We continue: Suppose there was some prime ideal $\mathfrak{q} \in \mathrm{Spec}(R)$ such that $\mathfrak{q} \neq 0$ and $\mathfrak{q} \notin \mathbb{V}(\mathfrak{a})_*$. In particular $u \in \mathfrak{q}$ and thereby $\mathfrak{a} \subseteq \mathfrak{q}$. Then due to (2.18.(iv)) there was a prime ideal minimal

over $\mathfrak{a}$, contained in $\mathfrak{q}$. By construction these ideals are the $\mathfrak{p}_i$ such that $0 \subset \mathfrak{a} \subseteq \mathfrak{p}_k \subset \mathfrak{q}$ for some $k \in 1 \ldots m$. The inclusion $\mathfrak{p}_k \subset \mathfrak{q}$ is strict, as $\mathfrak{q}$ is not one of the $\mathfrak{p}_i$. In particular we had $\operatorname{height}(\mathfrak{q}) \geq 2$. Taking $\mathfrak{b} := \mathfrak{q}$ and $n := \operatorname{height}(\mathfrak{b})$ there would be some $a_2, \ldots, a_n \in \mathfrak{q}$ such that $\operatorname{height}(\mathfrak{p}_2) = 2$ for some prime ideal $\mathfrak{p}_2 \trianglelefteq_{\mathfrak{i}} R$ minimal over $uR + a_2R$, according to (8.80.(v)). That is there is some ideal of height 2 containing $\mathfrak{a}$. Let us take this ideal for $\mathfrak{q}$, that is we may assume $\operatorname{height}(\mathfrak{q}) = 2$. Recall that by (8.84) the following set

$$\{\, \mathfrak{p}' \in \operatorname{Spec}(R) \mid 0 \subset \mathfrak{p}' \subset \mathfrak{q} \,\}$$

either is empty or infinite. As $\mathfrak{p}_k$ is contained in this set it is not empty and thereby infinite. In particular there is some $\mathfrak{p}'$ with $0 \subset \mathfrak{p}' \subset \mathfrak{q}$ that is none of the $\mathfrak{p}_i$, the prime ideals minimal over $\mathfrak{a}$. As $\mathfrak{p}' \neq 0$ we have $u \in \mathfrak{p}'$ and therefore $\mathfrak{a} \subseteq \mathfrak{p}'$ again. As before for $\mathfrak{q}$ we use (2.18.(iv)) to find a minimal prime ideal $\mathfrak{p}_j$ in between $\mathfrak{a} \subseteq \mathfrak{p}_j \subset \mathfrak{p}'$. Now we got

$$0 \subset \mathfrak{a} \subseteq \mathfrak{p}_j \subset \mathfrak{p}' \subset \mathfrak{q}$$

Thus we even have $\operatorname{height}(\mathfrak{q}) \geq 3$ in contradiction to $\operatorname{height}(\mathfrak{q}) = 2$. This contradiction can only be remedied if we could not have chosen $\mathfrak{q}$ in the first place. That is 0 and the $\mathfrak{p}_i$ where $i \in 1 \ldots m$ are the only prime ideals of R and this is a finite set.

- We have seen that $\operatorname{height}(\mathfrak{p}_i) = 1$ for any $i \in 1 \ldots n$. And as this are all the prime ideals (apart from 0), that R possesses, we conclude $\operatorname{kdim}(R) = 1$ - or R is a field already, in which case we get $\operatorname{kdim}(R) = 0$, as this was our first case.

- Let us begin with the equivalences of 1-dimensional noetherian integral domains: We have already seen (b) $\iff$ (d) above. But this time we also have $\operatorname{Spec}(R) = \operatorname{Smax}(R) \cup \{0\}$, as $\operatorname{kdim}(R) = 1$. Thus the Jacobson radical of R is just

$$\textsc{jac}(R) \;=\; \bigcap \operatorname{Smax}(R) \;=\; \bigcap \{\, \mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \neq 0 \,\}$$

Using (2.171.(i)) with this property we find that R is a Goldman domain, if and and only $\textsc{jac}(R) \neq 0$. Thus we also have (a) $\iff$ (d). Let us now prove (c) $\implies$ (d): Suppose R *was* a Goldman domain, as R also is a Hilbert domain, by assumption, R would be a field, because of (2.171.(ii)). But a field has $\operatorname{kdim}(R) = 0$ which is not the case, thus R cannot be a Goldman domain. Conversely for (d) $\implies$ (c): As R is not goldman, $R/0 = R$ is not a Goldman domain and this means $0 \trianglelefteq_{\mathfrak{i}} R$ is not a Goldman ideal. Any other prime ideal of R already is a maximal ideal, as $\operatorname{kdim}(R) = 1$. In particular any Goldman ideal of R is maximal and this means that R is a Hilbert domain.

□

Proof of (2.170):
The correct order of proofs is the following: Statements (i) and (ii) here are independent, but (iii) relies on (2.171) statements (i) to (iii). Thus these proofs have to be dealt with, first. Then again (2.171.(iv)) relies on (iii) here, so it is the capstone. We chose to present the statements ordered by themes, and apologize for the awkward order this inflicts on the proofs.

(i) Consider a Goldman ideal $\overline{\mathfrak{g}} \trianglelefteq_{\mathfrak{i}} \overline{R} := R/\mathfrak{a}$. Then by the correspondence theorem in quotient rings

$\overline{\mathfrak{g}}$ is of the form $\overline{\mathfrak{g}} = \mathfrak{g}/\mathfrak{a}$ for some ideal $\mathfrak{g} \trianglelefteq_{\mathrm{i}} R$ with $\mathfrak{a} \subseteq \mathfrak{g}$. As $\overline{\mathfrak{g}}$ is prime, so is $\mathfrak{g}$. The third isomorphism theorem yields

$$\overline{R}\Big/_{\overline{\mathfrak{g}}} \;=\; R/\mathfrak{a}\Big/_{\mathfrak{g}/\mathfrak{a}} \;\cong_{\mathrm{r}}\; R\Big/_{\mathfrak{g}}$$

As $\overline{\mathfrak{g}}$ is a Goldmann ideal, the quotient ring $\overline{R}/\overline{\mathfrak{g}}$ is a Goldman domain and by the above isomorphy this makes $R/\mathfrak{g}$ a Goldman domain. That is $\mathfrak{g}$ is a Goldman ideal, again. As R is a Hilbert ring, $\mathfrak{g}$ is maximal and by correspondence again this means $\overline{\mathfrak{g}}$ is maximal. As $\overline{\mathfrak{g}}$ was an arbitrary Goldman ideal of $R/\mathfrak{a}$ this makes $R/\mathfrak{a}$ a Hilbert ring.

(ii) If $\varphi : S \twoheadrightarrow R$ is an epimorphism of rings, then φ induces an isomorphism $\overline{\varphi} : S/\mathrm{kn}(\varphi) \xrightarrow{\sim} R$ of rings. But we assumed S to be a Hilbert ring and $\mathrm{kn}(\varphi) \trianglelefteq_{\mathrm{i}} R$ is an ideal. Thus $S/\mathrm{kn}(\varphi)$ is a Hilbert ring, by (i), too. And by the isomorphism $\overline{\varphi}$ we conclude, that R is a Hilbert ring, as well.

(iii) We will prove (1) in several steps: **Step 1:** Let $A = R[t]$ be the polynomial ring in one variable over R. We know R is a Hilbert ring and want to prove, that A is a Hilbert ring, too. So pick up any Goldman ideal $\mathfrak{h} \trianglelefteq_{\mathrm{i}} A$ and need to show that $\mathfrak{h}$ is maximal. **Step 1.1:** $\mathfrak{g} := \mathfrak{h} \cap R = 0$: As $\mathfrak{h}$ is a prime ideal, so is $\mathfrak{g}$. So in this case we already know that R is an integral domain. Suppose we had $\mathfrak{h} = 0$, then $R[t]/\mathfrak{h} = R[t]$ but by (2.167.(iii)) $R[t]$ is not a Goldman domain, whereas $R[t]/\mathfrak{h}$ is. Take $u := t + \mathfrak{h} \in R[t]/\mathfrak{h}$, then for any $f \in R[t]$ we get $f(u) = f(t) + \mathfrak{h} = f + \mathfrak{h}$ and therefore $R[u] = R[t]/\mathfrak{h}$. Also, as $\mathfrak{h} \neq 0$, there is some $h \in \mathfrak{h}$ such that $h \neq 0$. So for this h we get $h(u) = h + \mathfrak{h} = 0$, such that u is algebraic over R. Altogether $R[u]$ is algebraic and finitely generated over R and a Goldman domain. By (2.167.(vi)) this implies, that R is a Goldman domain. Yet R also is a Hilbert ring by assumption and using (2.171.(ii)) this implies R to be a field. That is u is integral over R and therefore $R[u] : R$ is an integral extension such that $R[u]$ is an integral domain and R is a field. Then (8.30.(viii)) tells us that $R[u] = R[t]/\mathfrak{h}$ is a field. This finally makes $\mathfrak{h}$ a maximal ideal, which had to be shown. **Step 1.2:** general $\mathfrak{g} := \mathfrak{h} \cap R$: Of course we have to reduce this to the case $\mathfrak{g} = 0$. By (i) we know that $\overline{R} := R/\mathfrak{g}$ is a Hilbert ring again. Now we regard everything inside the polynomial ring $\overline{R}[t]$ using the isomorphism in (3.43.(ii))

$$R\Big/_{\mathfrak{g}} \;\hookrightarrow\; R[t]\Big/_{\mathfrak{g}[t]} \;\cong_{\mathrm{r}}\; \Big(R\Big/_{\mathfrak{g}}\Big)[t]$$

As $\mathfrak{g}[t] = (\mathfrak{h} \cap R)R[t] \subseteq \mathfrak{h}$ we can regard the ideal $\overline{\mathfrak{h}} := \mathfrak{h}/\mathfrak{g}[t]$. And $\mathfrak{g}[t]$ corresponds to the zero-ideal of $\overline{R}[t]$. Also $\overline{R}[t]/\overline{\mathfrak{h}}$ is isomorphic to $R[t]/\mathfrak{h}$ due to the third isomorphism theorem. As $\mathfrak{h}$ is a Goldman ideal, $R[t]/\mathfrak{h}$ is a Goldman domain and hence $\overline{R}[t]/\overline{\mathfrak{h}}$ is a Goldman domain. So by step 1.1 above we conclude that $\overline{\mathfrak{h}}$ is a maximal ideal, but by correspondence, this means $\mathfrak{h}$ is a maximal ideal. As this is true for a general Goldman ideal $\mathfrak{h}$, we conclude that $R[t]$ is a Hilbert ring again. **Step 2:** By induction on n it is clear, that for any $n \in \mathbb{N}$ the polynomial ring $R[t_1, \ldots, t_n]$ is a Hilbert ring again. **Step 3:** If A is finitely generated, say $A = R[x_1, \ldots, x_n]$ for some $x_i \in A$, then we get an epimorphism of R-algebras $R[t_1, \ldots, t_n] \twoheadrightarrow A$ by $f \mapsto f(x_1, \ldots, x_n)$. As R is a Hilbert ring, so is $R[t_1, \ldots, t_n]$ by step 2. But by (ii) the image of a Hilbert ring is a Hilbert ring again, and A is such an image.

(iii) So let us prove properties (2) and (3) next: **Step 1:** $A = R[t_1, \ldots, t_n]$: Let us prove these properties by induction on n. In case $n = 0$ we have $A = R$ and hence $\mathfrak{m} = \mathfrak{n} \cap R = \mathfrak{n}$ is a maximal ideal

and thereby $[R/\mathfrak{n} : R/\mathfrak{m}] = 1$. Now for the induction step we have $B := R[t_1, \ldots, t_{n+1}]$ and let $A := R[t_1, \ldots, t_n]$ and $t := t_{n+1}$ such that $B = A[t]$. Consider any maximal ideal $\mathfrak{n} \trianglelefteq_{\mathrm{i}} B$ and let $\mathfrak{m} := \mathfrak{n} \cap A$. As $\mathfrak{n}$ is maximal (2.171.(iii)) tells us, that $\mathfrak{m}$ is a Goldman ideal. But R is a Hilbert ring, so A is a Hilbert ring, too. Therefore $\mathfrak{m}$ is a maximal ideal again. Thus by (2.168.(i)) $\mathfrak{n}$ is of the form $\mathfrak{n} = \mathfrak{m}[t] + fB$ for some monic polynomial $f \in A[t]$ such that $f + \mathfrak{m}[t]$ is a prime element of $B/\mathfrak{m}[t]$. Let us expand $B/\mathfrak{n}$ using the third isomorphism theorem

$$B\Big/_{\mathfrak{n}} \;=\; B\Big/_{\mathfrak{m}[t]+fB} \;\xrightarrow{\sim}\; A[t]/\mathfrak{m}[t]\Big/_{(\mathfrak{m}[t]+fB)/\mathfrak{m}[t]} \;:\; g+\mathfrak{n} \;\mapsto\; \big(g+\mathfrak{m}[t]\big)+\mathfrak{n}\Big/_{\mathfrak{m}[t]}$$

Then we can use the isomorphism $A[t]/\mathfrak{m}[t] \xrightarrow{\sim} (A/\mathfrak{m})[t]$ given by $g + \mathfrak{m}[t] \mapsto \overline{g} := \sum_k (g[k] + \mathfrak{m})t^k$. The ideal $\mathfrak{n}/\mathfrak{m}[t] = (\mathfrak{m}[t] + fB)/\mathfrak{m}[t]$ is mapped to $\overline{f}\,(A/\mathfrak{m})[t]$ and thereby we can reshape the above isomorphism into the form

$$B\Big/_{\mathfrak{n}} \;\xrightarrow{\sim}\; (A/\mathfrak{m})[t]\Big/_{\langle\overline{f}\rangle_{\mathrm{i}}} \;:\; g+\mathfrak{n} \;\mapsto\; \overline{g}+\mathfrak{n}\Big/_{\mathfrak{m}[t]}$$

Then by (8.10.(i)) $(A/\mathfrak{m})[t]/\langle\overline{f}\rangle_{\mathrm{i}}$ is finitely generated as an $(A/\mathfrak{m})$-vector space, the dimension being given to be $\deg(\overline{f}) = \deg(f)$, as f is monic. That is we have

$$\Big[B\Big/_{\mathfrak{n}} : A\Big/_{\mathfrak{m}}\Big] \;=\; \deg(f) \;<\; \infty$$

Now by induction hypothesis $\mathfrak{q} := \mathfrak{m} \cap R$ is a maximal ideal of R and $A/\mathfrak{m}$ and $A/\mathfrak{m}$ is a finite-dimensional $R/\mathfrak{q}$-vector space. Then we can use the degree formula (8.7.(iv)) to find

$$\Big[B\Big/_{\mathfrak{n}} : R\Big/_{\mathfrak{q}}\Big] \;=\; \Big[B\Big/_{\mathfrak{n}} : A\Big/_{\mathfrak{m}}\Big] \cdot \Big[A\Big/_{\mathfrak{m}} : R\Big/_{\mathfrak{q}}\Big] \;<\; \infty$$

Step 2: general A: By assumption $A = R[x_1, \ldots, x_n]$ is finitely generated and hence A is isomorphic to $R[t_1, \ldots, t_n]/\mathfrak{a}$ where the ideal $\mathfrak{a}$ is the kernel of $f \mapsto f(x_1, \ldots, x_n)$. Consider a maximal ideal $\overline{\mathfrak{n}} \trianglelefteq_{\mathrm{i}} R[t_1, \ldots, t_n]/\mathfrak{a}$, then $\overline{\mathfrak{n}}$ is of the form $\overline{\mathfrak{n}} = \mathfrak{n}/\mathfrak{a}$ for some maximal ideal $\mathfrak{n} \trianglelefteq_{\mathrm{i}} R[t_1, \ldots, t_n]$ with $\mathfrak{a} \subseteq \mathfrak{n}$. As $\mathfrak{n}$ is maximal step 1 yields, that $\mathfrak{m} := \mathfrak{n} \cap R$ is a maximal ideal again and that

$$\Big[R[t_1, \ldots, t_n]\Big/_{\mathfrak{n}} : R\Big/_{\mathfrak{m}}\Big] \;<\; \infty$$

Let us take a look at $\overline{\mathfrak{n}} \cap R$, that is the set of all $a \in R$ such that $a1_A = a(\mathbf{1} + \mathfrak{a}) \in \overline{\mathfrak{n}}$. But this is $a\mathbf{1} + \mathfrak{a} \in \mathfrak{n}/\mathfrak{a}$ which amounts to $a\mathbf{1} \in \mathfrak{n}$. But this is precisely the definition of $a \in \mathfrak{n} \cap R$ and thereby we have found the equality of

$$\overline{\mathfrak{n}} \cap R \;=\; \mathfrak{n} \cap R \;=\; \mathfrak{m}$$

In particular $\overline{\mathfrak{n}} \cap R$ is a maximal ideal of R. And as always the third isomorphism theorem turns $A/\overline{\mathfrak{n}}$ - which is given to be $(R[t_1, \ldots, t_n]/\mathfrak{a})/(\mathfrak{n}/\mathfrak{a})$ - into $R[t_1, \ldots, t_n]/\mathfrak{n}$. As this is an isomorphism of R-algebras, we find that we truly have a finite field extension

$$\Big[A\Big/_{\overline{\mathfrak{n}}} : R\Big/_{\mathfrak{m}}\Big] \;=\; \Big[R[t_1, \ldots, t_n]\Big/_{\mathfrak{n}} : R\Big/_{\mathfrak{m}}\Big] \;<\; \infty$$

□

Proof of (2.171):

(i) The equivalence (a) $\iff$ (b) is purely definitional: $0 \trianglelefteq_{\mathfrak{i}} R$ is a Goldman ideal, if and only if $R/0$ is a Goldman domain. But $R/0 = R$ is the same ring, naturally. For the other equivalences let us abbreviate $\mathcal{P} := \{\, \mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \neq 0 \,\}$ and $E := \operatorname{QUOT}(R)$ be the quotient field of R. The equivalence (a) $\iff$ (c) is easy: If R is goldman, then $E = R[1/u]$ for some $u \in R$ with $u \neq 0$. Thus by (2.167.(iii)) we have $u \in \bigcap \mathcal{P}$ and therefore $\bigcap \mathcal{P} \neq 0$. Conversely if $\bigcap \mathcal{P} \neq 0$ we can choose some $u \in \bigcap \mathcal{P}$ with $u \neq 0$ and find $E = R[1/u]$ by (2.167.(iii)) again.

In (a) $\implies$ (d) R is a Goldman domain. That is $E = R[1/u]$ for some $u \in R$ with $u \neq 0$. Thereby the following homomorphism of R-algebras is surjective

$$\varepsilon \;:\; R[t] \;\twoheadrightarrow\; E \;:\; f \mapsto f\left(\frac{1}{u}\right)$$

Let $\mathfrak{m} := \operatorname{kn}(\varepsilon)$ be the kernel of this homomorphism, then ε induces an isomorphism $R[t]/\mathfrak{m} \xrightarrow{\sim} E$. As E is a field, we conclude that $\mathfrak{m} \trianglelefteq_{\mathfrak{i}} R[t]$ is a maximal ideal. And if $a\mathbf{1} \in \mathfrak{m}$ then $0 = \varepsilon(1/u) = a\mathbf{1}(1/u) = a \cdot 1 = a$, such that $\mathfrak{m} \cap R = 0$.

Conversely for (c) $\implies$ (a) we let $u := t + \mathfrak{m} \in R[t]/\mathfrak{m}$. Then it is clear, that for any polynomial $f \in R[t]$ we get $f(u) = f(t + \mathfrak{m}) = f(t) + \mathfrak{m} = f + \mathfrak{m}$. In particular we have $R[u] = R[t]/\mathfrak{m}$ and $f(u) = 0$ is equivalent, to $f \in \mathfrak{m}$. As $\mathfrak{m}$ is a maximal ideal we have $\mathfrak{m} \neq 0$ - else $R[t]$ would be a field, but $t \in R[t]$ is not a unit. Thus we can choose some $f \in \mathfrak{m}$ with $f \in \mathfrak{m}$. And by the reasoning above, this means $f(u) = 0$. That is (1) $u \in R[t]/\mathfrak{m}$ is algebraic over R. Also, by construction, (2) $R[u]$ is finitely generated over R. As $R[u] = R[t]/\mathfrak{m}$ and $\mathfrak{m}$ is maximal, $R[u]$ is a field and hence (3) $R[u]$ is a Goldman domain. Due to properties (1) to (3) we conclude with (2.167.(v)) that R is a Goldman domain, too.

(ii) If F is a field, then F is a Goldman domain and $\operatorname{JAC}(F) = 0$, as 0 is the one and only maximal ideal of a field. Conversely suppose F is a Goldman domain satisfying $\operatorname{JAC}(F) = 0$. Then we have some $u \in F$ with $u \neq 0$ such that F_u is a field. Let $U := \{\, u^n \mid n \in \mathbb{N} \,\}$, that is $F_u = U^{-1}F$. Now consider any maximal ideal $\mathfrak{m}$ of F. Suppose we had $\mathfrak{m} \neq 0$, then there would be some $a \in \mathfrak{m}$ with $a \neq 0$ and hence $a/1 \in U^{-1}\mathfrak{m}$. But $a/1 \neq 0/1$ as $u \neq 0$ and F is an integral domain, such that $U^{-1}\mathfrak{m} \trianglelefteq_{\mathfrak{i}} F_u$ is non-zero. Yet F_u is a field, so any non-zero ideal has to be full $U^{-1}\mathfrak{m} = F_u$. Therefore $1/1 = m/u^n$ for some $m \in \mathfrak{m}$ which is $u^n \in \mathfrak{m}$. As $\mathfrak{m}$ is a prime ideal we conclude $n \neq 0$ and $u \in \mathfrak{m}$. Now, as $\mathfrak{m}$ has been an arbitrary maximal ideal of F, we have found $u \in \operatorname{JAC}(F)$ which equals 0 by assumption. Thus we have $u = 0$ in contradiction to $u \neq 0$ above. Thus the only maximal ideal of F is $\mathfrak{m} = 0$ and this means that F is a field.

- If F is a field, then F is a Goldman domain and the only prime ideal of F is 0. This is a Goldman ideal, but it also is maximal, hence F also is a Hilbert ring. Conversely suppose F is a Goldman domain and Hilbert ring. As R is an integral domain, $0 \trianglelefteq_{\mathfrak{i}} R$ is a prime ideal. And because of $R/0 = R$ we find that $R/0$ is a Goldman domain. This means 0 is a Goldman ideal and as R is a Hilbert ring, this means that 0 is maximal. But this is the case if and only if R is a field.

(iii) Property (b) is just a reformulation of (c) in (i) for the ring $R/\mathfrak{p}$: By the correspondence theorem of ideals in quotients (1.71) the prime ideals $\overline{\mathfrak{q}}$ of $\overline{R} := R/\mathfrak{p}$ are of the form $\overline{\mathfrak{q}} = \mathfrak{q}/\mathfrak{p}$ for some prime

ideal $\mathfrak{q} \trianglelefteq_{\mathrm{i}} R$ such that $\mathfrak{p} \subseteq \mathfrak{q}$. Thereby $\overline{\mathfrak{q}} \neq 0$ translates into $\mathfrak{p} \subset \mathfrak{q}$. Thus we get

$$\bigcap \{\, \overline{\mathfrak{q}} \in \operatorname{Spec}(\overline{R}) \mid \overline{\mathfrak{q}} \neq 0 \,\} \;=\; {\mathfrak{a}}\big/{\mathfrak{p}} \quad \text{for} \quad \mathfrak{a} := \bigcap \{\, \mathfrak{q} \in \operatorname{Spec}(R) \mid \mathfrak{p} \subset \mathfrak{q} \,\}$$

By (i) $\overline{R}$ is a Goldman domain, if and only if there is some $\overline{u} \in \mathfrak{a}/\mathfrak{p}$ with $\overline{u} \neq 0$. For $\overline{u} = u + \mathfrak{p}$ this translates into $u \in \mathfrak{a}$ with $u \notin \mathfrak{p}$. Thus $R/\mathfrak{p}$ is goldman, iff there is some $u \in \mathfrak{a} \setminus \mathfrak{p}$ and this is the equivalence of (a) and (b). In the next step we will prove the equivalence of (a) and (c):

- By (i) $\overline{R} := R/\mathfrak{p}$ is a Goldman domain if and only if there is some maximal ideal $\overline{\mathfrak{m}} \trianglelefteq_{\mathrm{i}} \overline{R}[t]$ such that $\overline{\mathfrak{m}} \cap \overline{R} = 0$. Using the isomorphism in (3.43.(ii)) we transfer $\overline{\mathfrak{m}}$ to a maximal ideal of $R[t]/\mathfrak{p}[t]$

$$\Phi \;:\; {R[t]}\big/{\mathfrak{p}[t]} \;\xrightarrow{\sim}\; \overline{R}[t] \;:\; f + \mathfrak{p}[t] \;\mapsto\; \sum_{k=0}^{\infty} \big(f[k] + \mathfrak{p}\big)\, t^k$$

That is we let $\mathfrak{m}/\mathfrak{p}[t] := \Phi^{-1}(\overline{\mathfrak{m}})$. Then $\overline{\mathfrak{m}}$ is a maximal ideal of $\overline{R}[t]$ if and only if $\mathfrak{m}$ is a maximal ideal of $R[t]$ - by the correspondence theorem of ideals, applied to $R[t]/\mathfrak{p}[t]$. Let us also verify that for this ideal we get

$$a \in \mathfrak{m} \cap R \quad\Longleftrightarrow\quad a + \mathfrak{p} \in \overline{\mathfrak{m}} \cap \overline{R}$$

By definition $a \in \mathfrak{m} \cap R$ is $a\mathbf{1} \in \mathfrak{m}$ and this of course is $a\mathbf{1} + \mathfrak{p}[t] \in \mathfrak{m}/\mathfrak{p}[t]$. As Φ is an isomorphism this again is $(a + \mathfrak{p})\mathbf{1} = \Phi(a\mathbf{1} + \mathfrak{p}[t]) \in \overline{\mathfrak{m}}$. Using the definition of the retraction again, this is $a + \mathfrak{p} \in \overline{\mathfrak{m}} \cap \overline{R}$. Starting with (a) there is such a maximal ideal $\overline{\mathfrak{m}}$ satisfying $\overline{\mathfrak{m}} \cap \overline{R} = 0$. And the construction above yields a maximal ideal $\mathfrak{m} \trianglelefteq_{\mathrm{i}} R[t]$ for which $a \in \mathfrak{m} \cap R$ is equivalent to $a + \mathfrak{p} \in \overline{\mathfrak{m}} \cap \overline{R} = 0 = \mathfrak{p}/\mathfrak{p}$. The latter is $a \in \mathfrak{p}$ and thereby $\mathfrak{m} \cap R = \mathfrak{p}$. Conversely, if we start with some maximal ideal $\mathfrak{m} \trianglelefteq_{\mathrm{i}} R[t]$ satisfying $\mathfrak{m} \cap R = \mathfrak{p}$ we have $\mathfrak{p}[t] = \mathfrak{p}R[t] = (\mathfrak{m} \cap R)R[t] \subseteq \mathfrak{m}$ and thereby can define $\overline{\mathfrak{m}} := \Phi(\mathfrak{m}/\mathfrak{p}[t])$. This is a maximal of $\overline{R}[t]$ and by the above we have $a + \mathfrak{p} \in \overline{\mathfrak{m}} \cap \overline{R}$ if and only if $a \in \mathfrak{m} \cap R = \mathfrak{p}$ which again is equivalent to $a + \mathfrak{p} = 0 \in \overline{R}$. Thus we have $\overline{\mathfrak{m}} \cap \overline{R} = 0$ and this makes $\overline{R} = R/\mathfrak{p}$ a Goldman domain.

(iv) Let us begin with (a) $\Longrightarrow$ (b): Given any prime ideal $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ we let $\mathfrak{a} := \bigcap \{\, \mathfrak{m} \in \operatorname{Smax}(R) \mid \mathfrak{p} \subseteq \mathfrak{m} \,\}$. Then $\mathfrak{p} \subseteq \mathfrak{a}$ is clear and we have to show, that even $\mathfrak{p} = \mathfrak{a}$. So suppose we had $u \in \mathfrak{a} \setminus \mathfrak{p}$ and let $U := \{\, u^n \mid n \in \mathbb{N} \,\}$. Then $\mathfrak{p} \cap U = \emptyset$ (as $\mathfrak{p}$ is prime) and hence we could choose a maximal element $\mathfrak{q}$ of $\{\, \mathfrak{b} \trianglelefteq_{\mathrm{i}} R \mid \mathfrak{p} \subseteq \mathfrak{b} \subseteq R \setminus U \,\}$ and by (2.18.(v)) $\mathfrak{q}$ is a prime ideal. Suppose $\mathfrak{q}$ was maximal, as $\mathfrak{p} \subseteq \mathfrak{q}$ and $u \in \mathfrak{a}$ this would imply $u \in \mathfrak{q}$, which is false. Hence $\mathfrak{q}$ is *not* a maximal ideal of R. However $\mathfrak{q}R_u$ is a maximal ideal of R_u by construction. Thus $R_u/\mathfrak{q}R_u$ is a field. But we have the following isomorphism

$$R_u \Big/ \mathfrak{q}R_u \;\xrightarrow{\sim}\; \Big(R \Big/ \mathfrak{q}\Big)_{u+\mathfrak{q}} \;:\; \frac{a}{u^n} + \mathfrak{q}R_u \;\mapsto\; \frac{a + \mathfrak{q}}{u^n + \mathfrak{q}}$$

according to (2.132.(ii)). But then, as $R_u/\mathfrak{q}R_u$ is a field, so is $(R/\mathfrak{q})_{u+\mathfrak{q}}$. But this means $\mathfrak{q}$ is a Goldman ideal of R and as $\mathfrak{q}$ is not maximal, R is not a Hilbert ring. Thus our assumption $u \notin \mathfrak{a} \setminus \mathfrak{p}$ had to be false and this means $\mathfrak{p} = \mathfrak{a}$, which is property (c) of Jacobson rings.

- Conversely for (b) $\Longrightarrow$ (a): If $\mathfrak{g} \trianglelefteq_{\mathrm{i}} R$ is a Goldman ideal, then by definition $R/\mathfrak{g}$ is a Goldman domain. But as R is jacobson by assumption, so is its quotient $R/\mathfrak{g}$, by (2.172.(i)). Now by (ii) together this implies $R/\mathfrak{g}$ to be a field, which in turn means, that $\mathfrak{g}$ is a maximal ideal. And as this

is true for any Goldman ideal, R is a Hilbert ring.

- The implication (a) $\implies$ (c) has already been done in property (2) of (2.170.(iii)). And (a) $\implies$ (d) is not far away either: If A is a finitely generated R-algebra it is isomorphic to a quotient of the polynomial ring $R[t_1,\ldots,t_n]/\mathfrak{n}$. And as A is assumed to be a field $\mathfrak{n} \trianglelefteq_{\mathrm{i}} R[t_1,\ldots,t_n]$ is a maximal ideal. So without loss of generality we may assume $A = R[t_1,\ldots,t_n]/\mathfrak{n}$. Let $\mathfrak{m} := \mathfrak{n} \cap R$, then $\mathfrak{m}$ is a maximal ideal, by property (2) of (2.170.(iii)). And by property (3) there A is a finite extension field of $R/\mathfrak{m}$. That is there is a finite $R/\mathfrak{m}$-basis $\{ x_1,\ldots,x_m \}$ of A (where $x_i = g_i + \mathfrak{n}$ for some $g_i \in R[t_1,\ldots,t_n]$) which means that any $f + \mathfrak{n} \in A$ can be expressed as a $R/\mathfrak{m}$-linear combination

$$f + \mathfrak{n} \;=\; \sum_{i=1}^{n} (a_i + \mathfrak{m})(g_i + \mathfrak{n}) \;=\; \sum_{i=1}^{n} a_i g_i + \mathfrak{n} \;=\; \sum_{i=1}^{n} a_i (g_i + \mathfrak{n})$$

 Thus the $R/\mathfrak{m}$-linear combination already is an R-linear combination and from this we find that the set $\{ x_1,\ldots,x_m \}$ also generates A as an R-module, so A is a finitely generated R-module.

- The implication (c) $\implies$ (a) is straightforward: Consider any Goldman ideal $\mathfrak{p}$ of R. By (iii) there is some maximal ideal $\mathfrak{m} \trianglelefteq_{\mathrm{i}} R[t]$ such that $\mathfrak{p} = \mathfrak{m} \cap R$. But by assumption (c) this implies that $\mathfrak{m} \cap R = \mathfrak{p}$ is maximal. As any Goldman ideal is maximal, R is a Hilbert ring.

- If remains to verify (d) $\implies$ (a), that is we have to verify that every Goldman ideal is maximal. Let us start with a Goldman ideal $\mathfrak{p}$, by (iii) this means there is some $u \in \mathfrak{a} \setminus \mathfrak{p}$ where $\mathfrak{a} := \bigcap \{ \mathfrak{q} \in \operatorname{Spec}(R) \mid \mathfrak{p} \subset \mathfrak{q} \}$. Let $x := u + \mathfrak{p}$ and $\overline{R} := R/\mathfrak{p}$ and distinguish two cases: **Case 1:** $\overline{R}_x$ is a field: As $\overline{R}_x = \overline{R}[1/x]$ is finitely generated over $\overline{R}$ it also is finitely generated over R by the same generating set $\{ 1/u \}$ - as before in (a) $\implies$ (c). By assumption (c), as $\overline{R}_x$ is a field, $\overline{R}_x : R$ is a finite ring extension and thereby integral - by (8.30.(v)). In turn this means that $\overline{R}_x : \overline{R}$ is an integral ring extension. But as $\overline{R}_x$ is a field and $\overline{R}$ is an integral domain this makes $\overline{R}$ a field, according to (8.30.(viii)). But this is the property desired: $\mathfrak{p}$ is a maximal ideal. **Case 2:** $\overline{R}_x$ is not a field: Then there is a maximal ideal $\overline{\mathfrak{n}} \trianglelefteq_{\mathrm{i}} \overline{R}_x$ that satisfies $\overline{\mathfrak{n}} \neq 0$. By the correspondence theorem of ideals in localisations (2.129) $\overline{\mathfrak{n}}$ corresponds to an ideal $\overline{\mathfrak{q}}$ in $\overline{R}$ maximal with the property $x \notin \overline{\mathfrak{q}}$. As $0 \trianglelefteq_{\mathrm{i}} \overline{R}_x$ corresponds to $0 \trianglelefteq_{\mathrm{i}} \overline{R}$ but $\overline{\mathfrak{n}} \neq 0$ we get $\overline{\mathfrak{q}} \neq 0$. And by (2.18.(v)) this $\overline{\mathfrak{q}}$ is prime. As before it is of the form $\overline{\mathfrak{q}} = \mathfrak{q}/\mathfrak{p}$ for some prime ideal $\mathfrak{q} \trianglelefteq_{\mathrm{i}} R$ with $\mathfrak{p} \subseteq \mathfrak{q}$. Hereby $\overline{\mathfrak{q}} \neq 0$ turns into $\mathfrak{p} \subset \mathfrak{q}$. And $x \notin \overline{\mathfrak{q}}$ turns into $u \notin \mathfrak{q}$. Altogether we have $\mathfrak{p} \subset \mathfrak{q} \in \operatorname{Spec}(R)$ and therefore $\mathfrak{a} \subseteq \mathfrak{q}$. But $u \in \mathfrak{a}$ such that $u \in \mathfrak{q}$ is a contradiction. Thus case 1 is the only one elegible, case 2 is void and we have proved that $\mathfrak{p}$ is maximal in case 1. So every Goldman ideal is maximal, which is the property of a Hilbert ring.

□

Proof of (2.172):

(ii) Suppose $(T,+,\cdot)$ is another integral domain and $\psi : S \twoheadrightarrow T$ a surjective homomorphism of rings. Then ψ can be composed with $\psi\varphi : R \twoheadrightarrow T$. As R is jacobson we get $\operatorname{JAC}(T) = 0$, by property (f) in the definition (2.33). As this is true for any ψ the same property implies S to be jacobson.

(i) Is an immediate consequence of (ii): It suffices to regard the canonical epimorphism $\varrho : R \twoheadrightarrow R/\mathfrak{a}$ given by $\varrho(a) := a + \mathfrak{a}$. As this is surjective and R is jacobson, so is $R/\mathfrak{a}$, according to (ii).

(vi) Let us denote $U := \{1, u, u^2, \dots\}$ that is $R_u = U^{-1}R$. By the correspondence theorem of ideals in localisations (2.129) there is a one-to-one correspondence of the maximal ideals, given by

$$\begin{array}{rcl} \mathrm{Smax}(R_u) & \longleftrightarrow & \{\, \mathfrak{a} \trianglelefteq_{\mathrm{i}} R \mid \mathfrak{a} \cap U = \emptyset \,\}^* \\ \mathfrak{n} & \mapsto & \mathfrak{n} \cap R \\ \mathfrak{a} R_u & \hookleftarrow & \mathfrak{a} \end{array}$$

If $\mathfrak{m}$ is a maximal ideal with $u \notin \mathfrak{m}$, then $\mathfrak{m}$ already is a maximal element among the $\mathfrak{a}$ with $\mathfrak{a} \cap U = \emptyset$: First of all $1 \notin \mathfrak{m}$, as $\mathfrak{m}$ is proper. Maximal ideals are prime and hence $u^n \in \mathfrak{m}$ would imply $u \in \mathfrak{m}$, which is not. Hence we have $\mathfrak{m} \cap U = \emptyset$. If now $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ with $\mathfrak{a} \cap U = \emptyset$ and $\mathfrak{m} \subseteq \mathfrak{a}$, then $\mathfrak{a}$ is proper, as $1 \notin \mathfrak{a}$ and hence $\mathfrak{m} = \mathfrak{a}$, as $\mathfrak{m}$ is a maximal ideal. Thus $\mathfrak{m}$ is a maximal element amongst the $\mathfrak{a}$ and hence we have an injective map

$$\{\, \mathfrak{m} \in \mathrm{Smax}(R) \mid u \notin \mathfrak{m} \,\} \;\hookrightarrow\; \mathrm{Smax}(R_u) \;:\; \mathfrak{m} \mapsto \mathfrak{m} R_u$$

That's it for general rings. For Jacobson rings we are able to prove, that this map also is surjective: Consider any maximal ideal $\mathfrak{n} \trianglelefteq_{\mathrm{i}} R_u$, then by (2.129) there is a *prime* ideal $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ with $\mathfrak{p} \cap U = \emptyset$, such that $\mathfrak{n} = \mathfrak{p}_u$ where $\mathfrak{p}_u := \mathfrak{p} R_u$. As R is jacobson we have

$$\mathfrak{p} \;=\; \bigcap \{\, \mathfrak{m} \in \mathrm{Smax}(R) \mid \mathfrak{p} \subseteq \mathfrak{m} \,\}$$

As $u \notin \mathfrak{p}$ there has to be some maximal ideal $\mathfrak{m}$ with $\mathfrak{p} \subseteq \mathfrak{m}$ but $u \notin \mathfrak{m}$. As before this means $\mathfrak{m} \cap U = \emptyset$. Now $\mathfrak{p} \subseteq \mathfrak{m}$ implies $\mathfrak{n} = \mathfrak{p}_u \subseteq \mathfrak{m}_u \neq R_u$. Suppose we had $1/1 \in \mathfrak{m}_u$ then there were some $m \in \mathfrak{m}$ and $k \in \mathbb{N}$ such that $1/1 = m/u^k$ which is $u^{k+j} = u^j m$ for some $j \in \mathbb{N}$. But as $u^{k+j} \notin \mathfrak{m}$, this cannot be. Hence $\mathfrak{m}_u$ is proper and as $\mathfrak{n}$ is maximal, this implies $\mathfrak{n} = \mathfrak{m}_u$. That is $\mathfrak{m} \mapsto \mathfrak{n}$ and hence the surjectivity.

- Consider any prime ideal $\mathfrak{q} \trianglelefteq_{\mathrm{i}} R_u$ then we have to prove that $\mathfrak{q}$ is the intersection of all maximal ideals $\mathfrak{n} \trianglelefteq_{\mathrm{i}} R_u$ containing $\mathfrak{q} \subseteq \mathfrak{n}$. But by the correspondence theorem (2.129) there is a prime ideal $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ with $u \notin \mathfrak{p}$ such that $\mathfrak{q} = \mathfrak{p}_u$. And by the above there is a maximal ideal $\mathfrak{m} \trianglelefteq_{\mathrm{i}} R$ such that $u \notin \mathfrak{m}$ such that $\mathfrak{n} = \mathfrak{m}_u$. That is we have to prove

$$\mathfrak{p}_u \;=\; \bigcap \{\, \mathfrak{m}_u \in \mathrm{Smax}(R_u) \mid \mathfrak{p}_u \subseteq \mathfrak{m}_u \,\}$$

As the intersection runs over maximal (hence prime) ideals satisfying $\mathfrak{m} \cap U = \emptyset$ it interchanges with the localisation U^{-1} according to (2.127). Thus due to the correspondence it suffices to verify the following identity in the base ring R

$$\mathfrak{p} \;=\; \bigcap \{\, \mathfrak{m} \in \mathrm{Smax}(R) \mid \mathfrak{p} \subseteq \mathfrak{m},\, u \notin \mathfrak{m} \,\}$$

As R is jacobson we know that $\mathfrak{p}$ is the intersection of *all* maximal ideals $\mathfrak{m}$ containing $\mathfrak{p} \subseteq \mathfrak{m}$. The above set is a subset of this and hence we have $\mathfrak{p} = \bigcap \{\, \mathfrak{m} \mid \mathfrak{p} \subseteq \mathfrak{m} \,\} \subseteq \bigcap \{\, \mathfrak{m} \mid \mathfrak{p} \subseteq \mathfrak{m}, u \notin \mathfrak{m} \,\}$. It remains to check the converse inclusion: Consider any $a \in R$ that is contained in any $\mathfrak{m}$ of the form $\mathfrak{p} \subseteq \mathfrak{m}$ and $u \notin \mathfrak{m}$. Suppose we had $a \notin \mathfrak{p}$ then there would have to be some $\mathfrak{m}$ with $\mathfrak{p} \subseteq \mathfrak{m}$ such that $a \notin \mathfrak{m}$ and $u \in \mathfrak{m}$. But then $au \in \mathfrak{m}$ for any $\mathfrak{m}$ with $u \in \mathfrak{m}$ and also $au \in \mathfrak{m}$ for any $\mathfrak{m}$

with $\mathfrak{p} \subseteq \mathfrak{m}$ and $u \notin \mathfrak{m}$, by assumption. Hence

$$au \in \left(\bigcap_{\substack{\mathfrak{p} \subseteq \mathfrak{m} \\ u \notin \mathfrak{m}}} \mathfrak{m} \right) \cap \left(\bigcap_{u \in \mathfrak{m}} \mathfrak{m} \right) \subseteq \bigcap_{\mathfrak{p} \subseteq \mathfrak{m}} \mathfrak{m} = \mathfrak{p}$$

As $au \in \mathfrak{p}$, $\mathfrak{p}$ is prime and $u \notin \mathfrak{p}$ we conclude $a \in \mathfrak{p}$. But this is the converse inclusion and hence we have the above equality for $\mathfrak{p}$ as an intersection. This yields the above equality for $\mathfrak{p}_u$ and this is the Jacobson property for R_u.

(iii) Let us first regard the case that S is a Jacobson ring, then we prove, that R is a Jacobson ring, too: To do this we have to regard any prime ideal $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ and have to show

$$\mathfrak{p} = \mathfrak{a} \quad \text{where} \quad \mathfrak{a} := \bigcap \{ \mathfrak{m} \in \operatorname{Smax}(R) \mid \mathfrak{p} \subseteq \mathfrak{m} \}$$

As $\mathfrak{p} \subseteq \mathfrak{a}$ is clear it suffices to check the converse inclusion: That is we assume $u \in \mathfrak{a} \setminus \mathfrak{p}$ and and aim for a contradiction. By the lying-over theorem (8.32.(i)) there is a prime ideal $\mathfrak{q} \trianglelefteq_{\mathrm{i}} S$ such that $\mathfrak{p} = \mathfrak{q} \cap R = \alpha^{-1}(\mathfrak{q}) = \{ a \in R \mid a1_S \in \mathfrak{q} \}$. As S is a Jacobson ring, we have

$$\mathfrak{q} = \mathfrak{b} \quad \text{where} \quad \mathfrak{b} := \bigcap \{ \mathfrak{n} \in \operatorname{Smax}(S) \mid \mathfrak{q} \subseteq \mathfrak{n} \}$$

If we had $u1_S \in \mathfrak{q}$, then $u \in \mathfrak{q} \cap R = \mathfrak{p}$, which is not the case and therefore $u1_S \notin \mathfrak{q}$. As $\mathfrak{q} = \mathfrak{b}$ there has to be some $\mathfrak{n} \in \operatorname{Smax}(S)$ with $\mathfrak{q} \subseteq \mathfrak{n}$ and $u1_S \notin \mathfrak{n}$. Let $\mathfrak{m} := \mathfrak{n} \cap R$, which is a maximal ideal of R, due to (8.32.(ii)). The inclusion $\mathfrak{q} \subseteq \mathfrak{n}$ also implies $\mathfrak{p} = \mathfrak{q} \cap R \subseteq \mathfrak{n} \cap R = \mathfrak{m}$ By definition $u \in \mathfrak{m}$ would mean $u1_S \in \mathfrak{n}$, which is not the case, therefore $u \notin \mathfrak{m}$. But as $\mathfrak{p} \subseteq \mathfrak{m}$ and $\mathfrak{m}$ is a maximal ideal, this contradicts $u \in \mathfrak{a}$ and hence there cannot be some $u \in \mathfrak{a} \setminus \mathfrak{p}$, such that $\mathfrak{a} \subseteq \mathfrak{p}$, too.

- Consider any prime ideal $\mathfrak{q} \trianglelefteq_{\mathrm{i}} S$, we have to prove, that $\mathfrak{q} = \mathfrak{b}$ where $\mathfrak{b} := \bigcap \{ \mathfrak{n} \in \operatorname{Smax}(S) \mid \mathfrak{q} \subseteq \mathfrak{n} \}$. Thereby it is clear, that $\mathfrak{q} \subseteq \mathfrak{b}$ as any $\mathfrak{n}$ contains $\mathfrak{q}$. Take $\mathfrak{p} := \mathfrak{q} \cap R$, then $\mathfrak{p}$ is a prime ideal, as $\mathfrak{q}$ was some. Now define

$$\mathcal{M} := \{ \mathfrak{m} \in \operatorname{Smax}(R) \mid \mathfrak{p} \subseteq \mathfrak{m} \} \quad \text{and} \quad \mathfrak{a} := \bigcap \mathcal{M}$$

As R is jacobson, by assumption, we have $\mathfrak{p} = \mathfrak{a}$. Next we aim to prove $\mathfrak{a} = \mathfrak{b} \cap R$, so let us take a look at the pull back of $\mathfrak{b}$: As $\mathfrak{n} \cap R = \alpha^{-1}(\mathfrak{n})$ is the pre-image of $\mathfrak{n}$ this operation commutes with intersections - according to (0.7) - and hence

$$\mathfrak{b} \cap R = \bigcap \mathcal{N} \quad \text{where} \quad \mathcal{N} := \{ \mathfrak{n} \cap R \mid \mathfrak{n} \in \operatorname{Smax}(S), \mathfrak{q} \subseteq \mathfrak{n} \}$$

For $\mathfrak{a} \subseteq \mathfrak{b} \cap R$ we start with some $a \in \mathfrak{a}$ and have to prove $a \in \mathfrak{n} \cap R$ for any $\mathfrak{n} \cap R \in \mathcal{N}$. As $\mathfrak{n} \trianglelefteq_{\mathrm{i}} S$ is maximal and $S : R$ is integral $\mathfrak{m} := \mathfrak{n} \cap R$ is maximal, too - due to lying-over (8.32.(ii)). And from $\mathfrak{q} \subseteq \mathfrak{n}$ we clearly get $\mathfrak{p} = \mathfrak{q} \cap R \subseteq \mathfrak{n} \cap R = \mathfrak{m}$ such that $\mathfrak{m} \in \mathcal{M}$. As $a \in \mathfrak{a} = \bigcap \mathcal{M} \subseteq \mathfrak{m}$ we conclude $a \in \mathfrak{m}$. As this is true for any $\mathfrak{n} \cap R$ we have $a \in \mathfrak{b} \cap R$, and $\mathfrak{a} \subseteq \mathfrak{b} \cap R$, as a has been arbitrary.

Conversely for $\mathfrak{b} \cap R \subseteq \mathfrak{a}$ we start with some $a \in \mathfrak{b} \cap R$ and have to show $a \in \mathfrak{m}$ for any $\mathfrak{m} \in \mathcal{M}$.

If $\mathfrak{p}$ is maximal itself, then $\mathfrak{q}$ is maximal, by (8.32.(ii)) such that $\mathcal{N} = \{\mathfrak{q} \cap R\} = \{\mathfrak{p}\} = \mathcal{M}$. In particular $\mathfrak{b} \cap R = \mathfrak{a}$ in this case. If $\mathfrak{p}$ is not maximal then any $\mathfrak{m} \in \mathcal{M}$ gives rise to a CPI $\mathfrak{p} \subset \mathfrak{m}$. As we have $\mathfrak{p} = \mathfrak{q} \cap R$ we can use going up (8.72.(ii)) to find a CPI $\mathfrak{q} \subset \mathfrak{n}$ with $\mathfrak{n} \cap R = \mathfrak{m}$. As $\mathfrak{m}$ is maximal, so is $\mathfrak{n}$ by (8.32.(ii)) again. Thus we have $\mathfrak{n} \cap R \in \mathcal{N}$ and therefore $a \in \mathfrak{b} \cap R = \bigcup \mathcal{N} \subseteq \mathfrak{n} \cap R$, which implies $a \in \mathfrak{n} \cap R = \mathfrak{m}$. Again, as $a \in \mathfrak{m}$ is true for any $\mathfrak{m} \in \mathcal{M}$ we get $a \in \mathfrak{a}$ and as $a \in \mathfrak{b} \cap R$ was arbitrary, we also conclude $\mathfrak{b} \cap R \subseteq \mathfrak{a}$.

Now that we have $\mathfrak{a} = \mathfrak{b} \cap R$ we are almost done: Recall that $\mathfrak{q} \subseteq \mathfrak{b}$ and we have just seen $\mathfrak{q} \cap R = \mathfrak{p} = \mathfrak{a} = \mathfrak{b} \cap R$. Also $\mathfrak{p}$ is prime such that by (8.32.(iv)) we conclude $\mathfrak{q} = \mathfrak{b}$, which was required for R to be a Jacobson ring.

□

Proof of (8.88):

(i) By definition the closure of P is the intersection of all closed sets of X containing P. The closed sets of X are of the form $\mathbb{V}(\mathfrak{a})$ for some ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$. That is we have

$$\overline{P} \;=\; \bigcap \{\, \mathbb{V}(\mathfrak{a}) \mid \mathfrak{a} \trianglelefteq_{\mathrm{i}} R,\, P \subseteq \mathbb{V}(\mathfrak{a}) \,\}$$

Hereby $P \subseteq \mathbb{V}(\mathfrak{a})$ translates into: For any $\mathfrak{p} \in P$ we have $\mathfrak{a} \subseteq \mathfrak{p}$. Thus if $P \subseteq \mathbb{V}(\mathfrak{a})$ then $\mathfrak{a} \subseteq \mathbb{I}(P)$. And conversely if $\mathfrak{a} \subseteq \mathbb{I}(P)$ then $\mathbb{V}\mathbb{I}(P) \subseteq \mathbb{V}(\mathfrak{a})$, as $\mathbb{V}$ is order reversing. But also any $\mathfrak{p} \in P$ satisfies $\mathbb{I}(P) \subseteq \mathfrak{p}$ and thereby $P \subseteq \mathbb{V}\mathbb{I}(P) \subseteq \mathbb{V}(\mathfrak{a})$. That is $P \subseteq \mathbb{V}(\mathfrak{a})$ and $\mathfrak{a} \subseteq \mathbb{I}(P)$ are equivalent and thus we have found

$$\overline{P} \;=\; \bigcap \{\, \mathbb{V}(\mathfrak{a}) \mid \mathfrak{a} \trianglelefteq_{\mathrm{i}} R,\, \mathfrak{a} \subseteq \mathbb{I}(P) \,\}$$

So clearly $\mathfrak{a} = \mathbb{I}(P)$ is part of the intersection and thereby $\overline{P} \subseteq \mathbb{V}(\mathbb{I}(P))$. If conversely $\mathfrak{a} \subseteq \mathbb{I}(P)$, then $\mathbb{V}\mathbb{I}(P) \subseteq \mathbb{V}(\mathfrak{a})$, as $\mathbb{V}$ is order-reversing. As this is true for any $\mathfrak{a}$ we have $\mathbb{V}\mathbb{I}(P) \subseteq \overline{P}$ such that these sets are equal.

(ii) If $\mathfrak{m} \in \mathrm{Smax}(R)$ is a maximal ideal, then there is no proper ideal (apart from $\mathfrak{m}$ itself) containing $\mathfrak{m}$ - this is what being maximal is all about. Thus we have $\mathbb{V}(\mathfrak{m}) = \{\mathfrak{m}\}$. And as set of the form $\mathbb{V}(\mathfrak{m})$ are closed by definition, $\mathfrak{m}$ is a closed point. Conversely let $\mathfrak{p} \in X$ be a closed point, that is $\{\mathfrak{p}\}$ is closed. Then the closure of $\{\mathfrak{p}\}$ is $\{\mathfrak{p}\}$ again. But by (i) the closure of $\{\mathfrak{p}\}$ is given to be

$$\{\mathfrak{p}\} \;=\; \overline{\{\mathfrak{p}\}} \;=\; \mathbb{V}\big(\mathbb{I}(\{\mathfrak{p}\})\big) \;=\; \mathbb{V}(\mathfrak{p})$$

Let $\mathfrak{m} \in \mathrm{Smax}(R)$ be a maximal ideal containing $\mathfrak{p} \subseteq \mathfrak{m}$, then $\mathfrak{m} \in \mathbb{V}(\mathfrak{p}) = \{\mathfrak{p}\}$ and hence $\mathfrak{m} = \mathfrak{p}$. In particular $\mathfrak{p}$ is maximal, itself.

(iii) Let us first check $B(a) = X \setminus \mathbb{V}(aR)$: If $\mathfrak{p} \in X$ such that $a \notin \mathfrak{p}$ then $a \in aR \subseteq \mathfrak{p}$ is false, such that $\mathfrak{p} \notin \mathbb{V}(aR)$. Conversely if $aR \subseteq \mathfrak{p}$ is false, then there is some $b \in R$ such that $ab \notin \mathfrak{p}$. In particular $a \notin \mathfrak{p}$, as $\mathfrak{p}$ is an ideal. Now that $B(a) = X \setminus \mathbb{V}(aR)$, we see that $B(a)$ is open. Also $B(1) = X$, as $1 \in \mathfrak{p}$ would imply $\mathfrak{p} = R$. Also for any a, $b \in R$ and any $\mathfrak{p} \in X$ we have $ab \in \mathfrak{p}$ equivalent to $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, as $\mathfrak{p}$ is a prime ideal. The negation thereof is $ab \notin \mathfrak{p}$ respectively

$a \notin \mathfrak{p}$ and $b \notin \mathfrak{p}$. Thus we have the identity

$$B(a) \cap B(b) \;=\; B(ab)$$

Thus $\mathcal{B}$ is the base of a topology on X. Let us check, that this is the Zariski-topology: Consider any open set $U = X \setminus \mathbb{V}(\mathfrak{a})$, then we will argue, that

$$U \;=\; \bigcup_{a \in \mathfrak{a}} B(a)$$

If $\mathfrak{p} \in U$ then $\mathfrak{a} \subseteq \mathfrak{p}$ is false. That is there is some $a \in \mathfrak{a}$ with $a \notin \mathfrak{p}$ and this is $\mathfrak{p} \in B(a)$. Conversely if $\mathfrak{p} \in B(a)$ for some $a \in \mathfrak{a}$, then for the same reason $\mathfrak{a} \subseteq \mathfrak{p}$ is false, such that $\mathfrak{p} \in U$.

(iv) Suppose there is some $a \in \mathfrak{p}$ such that $a \notin \mathfrak{q}$, then we have $\mathfrak{q} \in B(a)$ and $\mathfrak{p} \notin B(a)$. Thus by taking $U = B(a)$ we are done. If there is no such a, then $\mathfrak{p} \subseteq \mathfrak{q}$. Yet as $\mathfrak{p} \neq \mathfrak{q}$ this means $\mathfrak{p} \subset \mathfrak{q}$. In particular there is some $b \in \mathfrak{q}$ with $b \notin \mathfrak{p}$. Thus by $U := B(b)$ we get $\mathfrak{p} \in U$ and $\mathfrak{q} \notin B(b)$ and hence can close this case, too.

(v) To say $U_i \subseteq X$ is open, means that there is an ideal $\mathfrak{a}_i \trianglelefteq_{\mathfrak{i}} R$, such that $U_i = X \setminus \mathbb{V}(\mathfrak{a}_i)$. By assumption the U_i cover X and thereby we can compute

$$X \;=\; \bigcup_{i \in I} U_i \;=\; \bigcup_{i \in I} X \setminus \mathbb{V}(\mathfrak{a}_i) \;=\; X \setminus \bigcap_{i \in I} \mathbb{V}(\mathfrak{a}_i) \;=\; X \setminus \mathbb{V}\left(\sum_{i \in I} \mathfrak{a}_i \right)$$

Let us abbreviate the sum of the $\mathfrak{a}_i$ by $\mathfrak{a}$. Then the above identity means $\mathbb{V}(\mathfrak{a}) = \emptyset$. If we had $\mathfrak{a} \neq R$, then there was a maximal ideal $\mathfrak{m} \trianglelefteq_{\mathfrak{i}} R$ containing $\mathfrak{a} \subseteq \mathfrak{m}$. In particular $\mathfrak{m} \in \mathbb{V}(\mathfrak{a}) = \emptyset$, a contradiction. Thus we find $\mathfrak{a} = R$ and hence $1 \in \mathfrak{a}$. By construction this means that there is a finite subset $\Omega = \{ i(1), \ldots, i(n) \} \subseteq I$ such that $1 = a_{i(1)} + \cdots + a_{i(n)}$ for some $a_{i(k)} \in \mathfrak{a}_{i(k)}$. But then any ideal containing $a_{i(1)} + \cdots + a_{i(n)}$ would contain 1 and hence $\mathbb{V}(a_{i(1)} + \cdots + a_{i(n)}) = \emptyset$. From this we can return in a like manner

$$X \;=\; X \setminus \emptyset \;=\; X \setminus \mathbb{V}\left(\sum_{i \in \Omega} \mathfrak{a}_i \right) \;=\; X \setminus \bigcap_{i \in \Omega} \mathbb{V}(\mathfrak{a}_i) \;=\; \bigcup_{i \in \Omega} X \setminus \mathbb{V}(\mathfrak{a}_i) \;=\; \bigcup_{i \in \Omega} U_i$$

(vi) If $\mathfrak{u} \in \operatorname{Spec}(S)$ is a prime ideal, then $\varphi^{-1}(\mathfrak{u})$ is a prime ideal of R, as we have seen in (2.17). Also if $C := \mathbb{V}(\mathfrak{a})$ is a closed set of X, then $\varphi_*^{-1}(C) = \mathbb{V}(\mathfrak{u})$, where $\mathfrak{u} := \mathfrak{a}S$ is the ideal of S generated by $\varphi(\mathfrak{a})$. This has been shown in (2.17), as well. In particular $\varphi_*^{-1}(C) \subseteq Y$ is closed again and hence φ_* is a continuous map.

(vii) By (vi) the canonical map $\varrho : R \twoheadrightarrow R/\mathfrak{a} : b \mapsto b + \mathfrak{a}$ induces a continuous map ϱ^* on the spectra. And this is given to be $\varrho^{-1}(\mathfrak{p}/\mathfrak{a}) = \{ b \in R \mid b + \mathfrak{a} \in \mathfrak{p}/\mathfrak{a} \} = \{ b \in R \mid b \in \mathfrak{p} \} = \mathfrak{p}$. And from this it is clear, that ϱ^{-1} is injective. It remains to prove, that ϱ^{-1} also is closed: By the correspondence theorem (1.71) of ideals we have $\operatorname{Spec}(R/\mathfrak{a}) = \{ \mathfrak{p}/\mathfrak{a} \mid \mathfrak{p} \in \mathbb{V}(\mathfrak{a}) \}$. As the ideals of $R/\mathfrak{a}$ are of the form $\mathfrak{b}/\mathfrak{a}$ for some ideal $\mathfrak{b} \trianglelefteq_{\mathfrak{i}} R$ with $\mathfrak{a} \subseteq \mathfrak{b}$, a closed subset of $\operatorname{Spec}(R/\mathfrak{a})$ is of the form $\mathbb{V}(\mathfrak{b}/\mathfrak{a})$ and this is mapped to $\mathbb{V}(\mathfrak{b})$ under ϱ^*. In particular ϱ^* is a closed map, as well.

(viii) By (vi) the canonical map $\kappa : R \to U^{-1}R : a \mapsto a/1$ induces a continuous map κ^* on the spectra.

If $\widetilde{\mathfrak{p}}$ is an ideal of $U^{-1}R$ then it is of the form $\widetilde{\mathfrak{p}} = U^{-1}\mathfrak{p} = \{ p/u \mid p \in \mathfrak{p}, u \in U \}$ for some prime ideal $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ that satisfies $\mathfrak{p} \cap U = \emptyset$. This has been proved in (2.129). We then get $\kappa^*(\widetilde{\mathfrak{p}}) = \kappa^{-1}(\widetilde{\mathfrak{p}}) = \{ a \in R \mid a/1 \in \widetilde{\mathfrak{p}} \} = \{ a \in R \mid a \in \mathfrak{p} \} = \mathfrak{p}$. And from this it is clear that κ^* is injective. A general ideal of $U^{-1}R$ is of the form $\widetilde{\mathfrak{a}} = \{ a/u \mid a \in \mathfrak{a}, u \in U \}$ for some ideal $\mathfrak{a} \trianglelefteq_{\mathrm{i}} R$ (with $\mathfrak{a} = \mathfrak{a} : U$). Thus a closed set of $\mathrm{Spec}(U^{-1}R)$ is of the form $\mathbb{V}(\widetilde{\mathfrak{a}})$ and if $\widetilde{\mathfrak{p}}$ is a prime ideal of $U^{-1}R$ with $\widetilde{\mathfrak{a}} \subseteq \widetilde{\mathfrak{p}}$ then $\widetilde{\mathfrak{p}}$ is mapped to $\mathfrak{p}$ that satisfies $\mathfrak{a} \subseteq \mathfrak{p}$. Conversely if $\mathfrak{a} \subseteq \mathfrak{p}$ then $U^{-1}\mathfrak{a} \subseteq U^{-1}\mathfrak{p}$ such that $\kappa^*(\mathbb{V}(\widetilde{\mathfrak{a}}) = \mathbb{V}(\mathfrak{a})$, which means that κ^* is a closed map. Altogether κ^* is a homeomorphism, when restricted to its image.

□

Proof of (8.89):

(i) By construction $B(u) = X \setminus \mathbb{V}(uR)$ such that $B(v) \subseteq B(u)$ turns into $\mathbb{V}(uR) \subseteq \mathbb{V}(vR)$ and this again is $\mathbb{I}\{\,(\,\}\, vR) \subseteq \mathbb{IV}(uR)$. Thus we see $v \in \sqrt{vR} = \sqrt{uR}$ such that $v^n \in uR$ for some $n \in \mathbb{N}$. And this again means $v^n = up$ for some $p \in R$.

(ii) We have to check the well-definedness, the homomorphism property then is obvious from the construction. So consider any $a/u^r = b/u^s$, that is there is some $t \in \mathbb{N}$ such that $u^t u^s a = u^t u^r b$. Multiplying this equation by p^{r+s+t} we then get

$$p^{r+s+t}u^t u^s a \;=\; (up)^t (up)^s p^r a \;=\; v^{nt} v^{ns} p^r a$$

$$p^{r+s+t}u^t u^r b \;=\; (up)^t (up)^r p^s b \;=\; v^{nt} v^{nr} p^s b$$

As the left-hand side of these equations is identical, we get $p^r a/v^{nr} = p^s b/v^{ns}$ from the right-hand side, of these equations and this is the well-definedness of ϱ_u^v. Let us verify, that this homomorphism truly is independent of the choice of n and p. That is consider $v^{n_1} = up_1$ and $v^{n_2} = up_2$ then we have to verify (for any $a/u^m \in R_u$), that

$$\frac{ap_1^m}{v^{mn_1}} \;=\; \frac{ap_2^m}{v^{mn_2}}$$

Hence we regard

$$v^{mn_2} a p_1^m \;=\; (v^{n_2})^m a p_1^m \;=\; (up_2)^m a p_1^m \;=\; p_1^m p_2^m a u^m$$
$$v^{mn_1} a p_2^m \;=\; (v^{n_1})^m a p_2^m \;=\; (up_1)^m a p_2^m \;=\; p_1^m p_2^m a u^m$$

As the right-hand sides of these equations are identical, so are the left-hand sides, and from this we get $ap_1^m/v^{mn_1} = ap_2^m/v^{mn_2}$. Thus the construction of $\varrho_u^v(a/u^m)$ yields the same element of R_v regardless of the specific n and p chosen.

(iii) We will prove $\varrho_v^u \varrho_u^v(a/u^k) = a/u^k$ for any $a/u^k \in R_u$. That is $\varrho_v^u \varrho_u^v$ is the identity map of R_u and by the symmetry of the argument, we also find that $\varrho_u^v \varrho_v^u$ is the identity on R_v. To do this let $u^m = qv$ and $v^n = pu$, then we have to verify, that

$$\frac{a}{u^k} \;=\; \varrho_v^u \varrho_u^v \left(\frac{a}{u^k}\right) \;=\; \varrho_v^u \left(\frac{ap^k}{v^{km}}\right) \;=\; \frac{ap^k q^{kn}}{u^{knm}}$$

But this, we get from $u^{knm}a = (u^m)^{kn}a = (qv)^{kn}a = q^{kn}(v^n)^k a = q^{kn}(pu)^k a = u^k a p^k q^{kn}$. And in the localisation R_u this turns into the above identity $a/u^k = a^k q^{kn}/u^{knm}$ needed.

(iii) Now consider $B(w) \subseteq B(v) \subseteq B(u)$, then by (i) we find $v^m = pu$ and $w^n = qv$ for some m, $n \in \mathbb{N}$ and p, $q \in R$. From this we see $w^{mn} = q^m v^m = q^m pw$ such that ϱ_u^w can be described as

$$\varrho_u^w\left(\frac{a}{u^k}\right) \;=\; \frac{a(q^m p)^k}{(w^{mn})^k} \;=\; \frac{aq^{km}p^k}{w^{kmn}}$$

Comparing this to the composition $\varrho_v^w \varrho_u^v$ we find, that these maps are identical, as

$$\varrho_v^w \varrho_u^v\left(\frac{a}{u^k}\right) \;=\; \varrho_v^w\left(\frac{ap^k}{v^{km}}\right) \;=\; \frac{(ap^k)q^{km}}{v^{kmn}} \;=\; \varrho_u^w\left(\frac{a}{u^k}\right)$$

□

Proof of (8.90):

- (a) $\Longrightarrow$ (b) can be proved by induction on n: For $n = 1$ the claim is trivial, so consider $n \geq 2$ and define $C := C_1$ and $D := C_2 \cup \cdots \cup C_n$. Let us first assume $C = C_1 \cup \cdots \cup C_n = C \cup D$, then by the irreducibility of I it follows that $I = C$ or $I = D$. In the first case $I = C_1$ we are done. In the latter case $I = C_2 \cup \cdots \cup C_k$ we find some $k \in 2 \ldots n$ with $I = C_k$, by induction hypothesis. Together we have proved the induction step and hence (b).

- (b) $\Longrightarrow$ (c) is quite obvious: We start with $I \subseteq C_1 \cup \cdots \cup C_n$ for some closed sets $C_i \subseteq X$. In this case simply let $B_i := C_i \cap I$, which are closed subsets of I. Then we get $I = B_1 \cup \cdots \cup B_n$ and by assumption (b) there is some $k \in 1 \ldots n$ such that $I = B_k$. But from $I = B_k = C_k \cap I$ we conclude $I \subseteq C_k$ again, which is (c).

- For the converse direction (c) $\Longrightarrow$ (a) we consider closed subsets C, $D \subseteq I$ such that $I = C \cup D$. That is $C = C' \cap I$ resp. $D = D' \cap I$ for some closed sets C', $D' \subseteq X$. As $I = C \cup D = (C' \cap I) \cup (D' \cup I) = (C' \cup D') \cap I$ we have $I \subseteq C' \cup D'$ and hence by assumption (c), without loss of generality, $I \subseteq C'$. This again is $I = C' \cap I = C$.

- (a) $\Longrightarrow$ (d): Let $C := I \setminus U$ and $D := I \setminus V$, then C and D are closed subsets of I and since U and V are non-empty we have $C \neq I$ and $D \neq I$. Thus by (a) we have $I \neq B \cup C$, which yields the claim by going to complements

$$\emptyset \;=\; I \setminus I \;\neq\; I \setminus (C \cup D) \;=\; (I \setminus C) \cap (I \setminus D) \;=\; U \cap V$$

- (d) $\Longrightarrow$ (e): Let $V := I \setminus \overline{U}$ where $\overline{U}$ denotes the closure of U in I. Then clearly V is an open subset of I and we have $U \cap V = \emptyset$ (as $x \in V$ is just $x \notin \overline{U}$, in particular $x \notin U$ since $U \subseteq \overline{U}$). By (b) and the assumption $U \neq \emptyset$ we find $V = \emptyset$, which is $\overline{U} = I$.

- (e) $\Longrightarrow$ (d): Consider non-empty, open subsets U, $V \subseteq I$ and let $D := I \setminus V$. If $U \cap V = \emptyset$, then clearly $U \subseteq D$. But D is closed in I and $U \neq \emptyset$ by assumption, such that $D \neq \emptyset$, too. Now (c) implies that $D = I$ and hence $V = \emptyset$ in contradiction to V being non-empty.

- (d) $\implies$ (a): Suppose $I = C \cup D$ for some closed subsets $C, D \subseteq I$ and let $U := I \setminus C$ and $V := I \setminus D$. Then U and V are open subsets of I and $I = C \cap D$ yields $U \cap V = \emptyset$ by going to complements. Hence by (b) we get $U = \emptyset$ or $V = \emptyset$ and this is nothing but $C = I$ or $D = I$.

- Pick up any $x \in X$ and let $I_x := \overline{\{ x \}} \subseteq X$. By construction I_x is closed and we now prove, that I_x also is irreducible: Suppose $I_x = C \cup D$ for some closed subsets $C, D \subseteq I$. As $x \in I$ we have $x \in C$ or $x \in D$. Without loss of generality we assume $x \in C$, that is $\{ x \} \subseteq C$. As $C \subseteq I_x$ and $I_x \subseteq X$ are closed, so is $C \subseteq X$ and thereby $I_x = \overline{\{ x \}} \subseteq C \subseteq I_x$. That is $C = I_x$, which is the irreducibility of I_x.

- Let us now prove, that is a T_0-space we get $I_x = I_y \implies x = y$: Suppose $x \neq y$ then by assumption there is an open set $P \subseteq X$ such that $x \in P$ and $y \notin P$ (we may assume this without loss of generality, as the other case $y \in P$ and $x \notin P$ is analogous). Now let $C := I_y \setminus U$, then $\{ y \} \subseteq C$ and hence $x \in I_x = I_y \subseteq C$, as C is closed. But this yields $x \notin U$, a contradiction.

□

Proof of (8.91):

(i) (a) $\implies$ (b): Suppose $\overline{I} = C \cup D$ for some closed sets $C, D \subseteq \overline{I}$. Hence $C, D \subseteq X$ are closed, such that $C \cap I$ and $D \cap I \subseteq I$ are closed, too. Now regard

$$I \;=\; (C \cap I) \cup (D \cap I)$$

As both of these sets are closed and I was assumed to be irreducible, we may take (without loss of generality again) $I = C \cap I$. In other words $I \subseteq C \subseteq \overline{I}$. And from this we get $\overline{I} \subseteq \overline{C} = C \subseteq \overline{I}$ (where the closure is taken in X) which is $C = \overline{I}$ and hence $\overline{I}$ is irreducible.

- (b) $\implies$ (a): Suppose $I = C \cup D$ for some closed subsets $C, D \subseteq I$. Then the closure (in X) satisfies $\overline{I} = \overline{C \cup D} = \overline{C} \cup \overline{D}$. As $\overline{I}$ was assumed to be irreducible we may assume, without loss of generality, that $\overline{I} = \overline{C}$. But as C has been closed in I we have $C = I \cap \overline{C} = I \cap \overline{I} = I$, which means that I is irreducible.

- The implication (c) $\implies$ (a) is clear (just let $P := I$). For the converse implication (a) $\implies$ (c) consider any open subset $P \subseteq I$. If $\emptyset \neq P', P'' \subseteq P$ are open, then $\emptyset \neq P', P'' \subseteq I$ are open and hence $P' \cap P'' \neq \emptyset$, due to the irreducibility of I. But this means that P is irreducible.

(ii) We will prove this by zornification: Let $\mathcal{Z} := \{ J \in \mathcal{I}(X) \mid I \subseteq J \}$. In particular $\mathcal{Z} \neq \emptyset$ is non-empty, as $I \in \mathcal{Z}$. And $\mathcal{Z}$ is partially ordered under $\subseteq$. We will now prove, that every chain in $\mathcal{Z}$ has a maximal element: Suppose $(J_\lambda) \subseteq \mathcal{Z}$ (where $\lambda \in \Lambda$) is a chain of irreducible sets containing I. Then we let $J := \bigcup_\lambda J_\lambda$. Now consider some non-empty, open subsets $P, Q \subseteq J$ (that is $P = P' \cap J$ and $Q = Q' \cap J$ for some open subsets $P', Q' \subseteq X$). Then we let $P_\lambda := P' \cap J_\lambda$ and $Q_\lambda := Q' \cap J_\lambda$ which are open subsets of J_λ. It is clear that $\bigcup_\lambda P_\lambda = P' \cap J = P$ and $\bigcup_\lambda Q_\lambda = Q' \cap J = Q$ and also $P_\lambda \cap Q_\lambda = P' \cap Q' \cap J_\lambda \subseteq P' \cap Q' \cap J = P \cap Q$. As $P \neq \emptyset$ there has to be some $\lambda \in \Lambda$ such that $P_\lambda \neq \emptyset$ and likewise there is some $\mu \in \Lambda$ such that $Q_\mu \neq \emptyset$. As (J_λ) is a chain we may assume (without loss of generality) that $J_\lambda \subseteq J_\mu$. Now suppose $P \cap Q = \emptyset$ then also $P_\mu \cap Q_\mu = \emptyset$. But as J_μ is irreducible and $Q_\mu \neq \emptyset$, this can only be if $P_\mu = \emptyset$. As $J_\lambda \subseteq J_\mu$ this

implies $P_\lambda \subseteq P_\mu = \emptyset$, a contradiction. Hence $P \cap Q \neq \emptyset$ which means that J is irreducible and thereby $J \in \mathcal{Z}$ is an upper bound of (J_λ). Thus by the lemma of Zorn there is a maximal element $J \in \mathcal{Z}$ and being maximal means that $J \in \operatorname{IRR}(X)$ is an irreducible component.

(iii) Suppose I was *not* connected, then there would be a subset $C \subseteq I$ that is both open and closed and neither $\emptyset$ nor I. Let $D := I \setminus C$, as C is open, $D \subseteq I$ is closed. Also $D \neq I$, as $C \neq \emptyset$. But $I = C \cup D$ is clear and both C, $D \neq I$ this means that I is not irreducible.

(iv) Suppose $f(I) = C \cup D$ for some closed subsets C, $D \subseteq f(I)$. That is $C = C' \cap f(I)$ and $D = D' \cap f(I)$ for some closed subsets C' and $D' \subseteq Y$. Hence $f(I) \subseteq C' \cup D'$ which implies

$$I \subseteq f^{-1}(f(I)) \subseteq f^{-1}(C' \cup D') = f^{-1}(C') \cup f^{-1}(D')$$

As f is continuous and C', $D' \subseteq Y$ are closed, so are $f^{-1}(C')$ and $f^{-1}(D') \subseteq X$. But as I is irreducible property (d) in (i) implies, that (without loss of generality) $I \subseteq f^{-1}(C')$. Hence $f(I) \subseteq f(f^{-1}(C')) \subseteq C'$ which further implies $C \subseteq f(I) \subseteq C' \cap f(I) = C$, that is $f(I) = C$.

(v) Let us first prove, that $\{ x \}$ is closed: Consider any $y \in I_x := \overline{\{ x \}}$ and suppose $x \neq y$. Then - as X is hausdorff - there are open subsets U, $V \subseteq X$ such that $x \in U$, $y \in V$ and $U \cap V = \emptyset$. The $x \in I_x \setminus V$ which is a closed subset of X. As I_x is the smallest closed subset containing x this implies $I_x \setminus V = I_x$ and thereby $y \in I_x \setminus V$, contradicting $y \in V$. Thus y cannot be different from x and this means $I_x = \{ x \}$.

By (8.90) $I_x = \{ x \}$ is an irreducible set and hence, by (ii), there is an irreducible component $I \in \operatorname{IRR}(X)$ containing $I_x \subseteq I$. As before suppose there was some $y \in I$ with $y \neq x$. Then $x \in U$ and $y \in V$ for some open subsets U, $V \subseteq X$ with $U \cap V = \emptyset$. As $x \in U$ and $x \in I_x \subseteq I$ we get $I_x \subseteq U \cap I$, which is an open subset of I. Likewise $y \in V \cap I$ and as I is irreducible and U, V are non-empty, we would conclude $(U \cap I) \cap (V \cap I) \neq \emptyset$. But this contradicts $U \cap V = \emptyset$, such that y cannot be different from x. Again this means $I = \{ x \}$ and thereby $\{ x \}$ is an irreducible component of X.

Conversely, if we start with an irreducible component $I \in \operatorname{IRR}(X)$, then I cannot be $I = \emptyset$ as this would not be maximal. That is $x \in I$ for some $x \in X$ and thereby $\{ x \} \subseteq I$. But as $\{ x \}$ is an irreducible component - that is maximal - we conclude $\{ x \} = I$. That is there are no other irreducible components in X, apart from the one-point sets $\{ x \}$.

□

Proof of (8.93):
Consider any $x \in X$ then $x \in I_x := \overline{\{ x \}}$ and I_x is irreducible. Hence I_x is contained in some irreducible component $I_x \subseteq J \in \operatorname{IRR}(X)$. Therefore we get $x \in \bigcup \operatorname{IRR}(X)$, and as x has been arbitrary this proves $X = \bigcup \operatorname{IRR}(X)$. As $X \neq \emptyset$ is non-empty, there is some $x \in X$. Thus the empty set $\emptyset \subset I_x$ is irreducible, but not maximal. Hence $\emptyset \notin \operatorname{IRR}(X)$. Now consider any irreducible component $I \in \operatorname{IRR}(X)$. In particular I is irreducible, such that $\overline{I}$ is irreducible, too. But from $I \subseteq \overline{I}$ and the maximality of I we get $I = \overline{I}$, that is I is closed. Thus we have proved the first four claims.

If $\mathcal{I} = \operatorname{IRR}(X)$ is the set of irreducible components of X, then the properties (1) and (2) have just been proved. Now suppose $\mathcal{I} = \{ I_1, \ldots, I_r \}$ then we also get property (3): Without loss of generality we will

prove this for $I = I_1$. Suppose $I_1 \subseteq X = I_2 \cup \cdots \cup I_r$, as I_1 is irreducible and any I_j is closed there is some $k \in 2 \ldots r$ such that $I_1 \subseteq I_k$. By the maximality of I_1 this is $I_1 = I_k$, a contradiction. This yields $X \neq I_2 \cup \cdots \cup I_r$ which had to be proved.

Conversely suppose $\mathcal{I} = \{ I_1, \ldots, I_r \}$ is a set satisfying the properties (1), (2) and (3). If $J \in \operatorname{IRR}(X)$ is any irreducible component, then $J \subseteq X = I_1 \cup \cdots \cup I_r$ by (1). As J is irreducible and any I_j is closed by (2), this implies that $J \subseteq I_k$ for some $k \in 1 \ldots r$. But as I_k also is irreducible and J is maximal this yields $J = I_k \in \mathcal{I}$. Hence we have proved $\operatorname{IRR}(X) \subseteq \mathcal{I}$. Now suppose there was any $I \in \mathcal{I}$ that was no irreducible component $I \notin \operatorname{IRR}(X)$. As I is irreducible it is nevertheless contained in an irreducible component $I \subset J \in \operatorname{IRR}(X)$. Hence $X = \bigcup \operatorname{IRR}(X) = \bigcup \{ J \in \mathcal{I} \mid J \neq I \}$ in contradiction to property (3). Hence we truly have $\mathcal{I} = \operatorname{IRR}(X)$. □

Proof of (8.92):

(iii) Let $P := \{ \mathfrak{p} \}$, then $\mathbb{I}(P) = \bigcap P = \mathfrak{p}$ and thereby $\overline{P} = \mathbb{V}\mathbb{I}(P) = \mathbb{V}(\mathfrak{p})$. As the closure of a set that contains one point only is irreducible, by (8.90) we conclude that $\mathbb{V}(\mathfrak{p})$ is irreducible. And $\mathfrak{p}$ is the generic point of $\overline{P} = \mathbb{V}(\mathfrak{p})$, by definition. As $\mathbb{V}(\mathfrak{p})$ is closed, by definition of the Zariski-topology and $\mathfrak{p} \in \mathbb{V}(\mathfrak{p})$ makes $\mathbb{V}(\mathfrak{p})$ non-empty, this already is the implication (a) $\implies$ (b).

Conversely suppose I is non-empty, closed and irreducible. As I is closed, it is of the form $I = \mathbb{V}(\mathfrak{p})$ for some ideal $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$. It remains to prove, that $\mathfrak{p}$ is prime. Suppose we had $\mathfrak{p} = R$, then $I = \mathbb{V}(\mathfrak{p}) = \mathbb{V}(R) = \emptyset$, which was assumed to not be the case. Hence $\mathfrak{p} \neq R$ is a proper ideal. Also, if $a, b \in R$ with $ab \in \mathfrak{p}$, then we have $abR \subseteq \mathfrak{p}$ and thereby $\mathfrak{p} \in \mathbb{V}(abR) = \mathbb{V}(aR) \cup \mathbb{V}(bR)$ according to (2.16). In case $\mathfrak{p} \in \mathbb{V}(aR)$ we have $a \in aR \subseteq \mathfrak{p}$ and thereby $a \in \mathfrak{p}$. Likewise we get $b \in \mathfrak{p}$ in case $\mathfrak{p} \in \mathbb{V}(bR)$. That is $\mathfrak{p}$ truly is a prime ideal of R.

(i) If R is an integral domain, then the zero-ideal $0 \trianglelefteq_{\mathrm{i}} R$ is prime. Hence by (iii) we conclude that $\operatorname{Spec}(R) = \mathbb{V}(0)$ is an irreducible set with generic point 0. Let us also present a more algebraic proof of the statement:

Let us abbreviate $X := \operatorname{Spec}(R)$ and suppose $X = C \cup D$ for some closed subsets $C, D \subseteq X$. That is $C = \mathbb{V}(\mathfrak{a})$ and $D = \{ \} \mathbb{V}(\mathfrak{b})$ for some ideals $\mathfrak{a}, \mathfrak{b} \trianglelefteq_{\mathrm{i}} R$. Then

$$X \;=\; \mathbb{V}(\mathfrak{a}) \cup \mathbb{V}(\mathfrak{b}) \;=\; \mathbb{V}(\mathfrak{a} \cap \mathfrak{b})$$

That is for any prime ideal $\mathfrak{p}$ of R we have $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{p}$. As R is an integral domain, 0 is a prime ideal and from $\mathfrak{a} \cap \mathfrak{b} \subseteq 0$ we conclude $\mathfrak{a} \cap \mathfrak{b} = 0$. Now suppose there were some $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ with $a \neq 0$ and $b \neq 0$. As R is an integral domain, this would mean $ab \neq 0$, but also $ab \in \mathfrak{a} \cap \mathfrak{b} = 0$. This contradiction means we cannot have both, $a \neq 0$ and $b \neq 0$, and thereby $\mathfrak{a} = 0$ or $\mathfrak{b} = 0$. But from $\mathfrak{a} = 0$ we get $C = \mathbb{V}(\mathfrak{a}) = X$ and likewise $\mathfrak{b} = 0$ would mean $D = \mathbb{V}(\mathfrak{b}) = X$. That is X is irreducible. And as $\mathbb{I}(\{0\}) = \bigcap\{0\} = 0$ we also find, that

$$\overline{\{0\}} \;=\; \mathbb{V}\mathbb{I}(\{0\}) \;=\; \mathbb{V}(0) \;=\; X$$

(ii) Consider any two elements $a, b \in R$ such that $ab = 0$ and denote the ideals $\mathfrak{a} := aR$ and $\mathfrak{b} := bR$. Again abbreviate $X := \operatorname{Spec}(R)$, which is irreducible, by assumption. If $\mathfrak{p} \trianglelefteq_{\mathrm{i}} R$ is any prime ideal,

then we distinguish two cases: (1) If $a \in \mathfrak{p}$, then $\mathfrak{a} \subseteq \mathfrak{p}$ and hence $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a} \subseteq \mathfrak{p}$. (2) If $a \notin \mathfrak{p}$, then still $ab = 0 \in \mathfrak{p}$ such that $b \in \mathfrak{p}$. But this is $\mathfrak{b} \subseteq \mathfrak{p}$ and hence $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{b} \subseteq \mathfrak{p}$ again. Thus in both cases, we have $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{p}$ and thereby

$$X \;=\; \mathbb{V}(\mathfrak{a} \cap \mathfrak{b}) \;=\; \mathbb{V}(\mathfrak{a}) \cup \mathbb{V}(\mathfrak{b})$$

As X is irreducible, we may take $X = \mathbb{V}(\mathfrak{a})$ without loss of generality. That is $\mathfrak{a} \subseteq \mathfrak{p}$ for any prime ideal $\mathfrak{p} \trianglelefteq_{\mathfrak{i}} R$ and thereby

$$\mathfrak{a} \;\subseteq\; \bigcap \mathrm{Spec}(R) \;=\; \textsc{nil}(R) \;=\; 0$$

Thereby $\textsc{nil}(R) = 0$, as R was assumed to be reduced. That is $\mathfrak{a} = 0$ and this is $a = 0$. Thus from $ab = 0$ we conclude $a = 0$ (or $b = 0$ in case $X = \mathbb{V}(\mathfrak{b})$), that is R an integral domain.

(iv) If $I \in \textsc{irr}(X)$ is an irreducible component of $X = \mathrm{Spec}(R)$, then it already is non-empty, closed and irreducible, because of (8.93). Thus from (iii) we get $I = \mathbb{V}(\mathfrak{p})$ for some prime ideal $\mathfrak{p} \trianglelefteq_{\mathfrak{i}} R$. We have to show that $\mathfrak{p}$ is minimal, that is we assume $\mathfrak{q} \subseteq \mathfrak{p}$ for some $\mathfrak{q} \in X$. Then we would get $\mathbb{V}(\mathfrak{p}) \subseteq \mathbb{V}(\mathfrak{q})$ and as by (iii) $\mathbb{V}(\mathfrak{q})$ is irreducible and $\mathbb{V}(\mathfrak{p})$ is maximal by assumption, this would imply $\mathbb{V}(\mathfrak{p}) = \mathbb{V}(\mathfrak{q})$. In particular $\mathfrak{q} \in \mathbb{V}(\mathfrak{p})$, which is $\mathfrak{p} \subseteq \mathfrak{q}$ and thereby $\mathfrak{p} = \mathfrak{q}$.

Conversely, if $\mathfrak{p} \in \mathrm{Smin}(R)$ is a minimal prime ideal, then we know that $\mathbb{V}(\mathfrak{p})$ is irreducible, by (iii). It remains to prove that $\mathbb{V}(\mathfrak{p})$ is an irreducible component, that is we assume $\mathbb{V}(\mathfrak{p}) \subseteq J$ for some irreducible $J \subseteq X$. As $J \subseteq \overline{J}$ and $\overline{J}$ also is irreducible, by (8.91), we also get $\mathbb{V}(\mathfrak{p}) \subseteq \overline{J}$. As $\mathfrak{p} \in \mathbb{V}(\mathfrak{p})$ we also have $\mathfrak{p} \in \overline{J}$ and hence $\overline{J} \neq \emptyset$. Thus by (iii) we get $\overline{J} = \mathbb{V}(\mathfrak{q})$ for some prime ideal $\mathfrak{q} \in X$. Now $\mathfrak{p} \in \overline{J} = \mathbb{V}(\mathfrak{q})$ means $\mathfrak{q} \subseteq \mathfrak{p}$, but as $\mathfrak{p}$ is minimal, this means $\mathfrak{q} = \mathfrak{p}$ and thereby $\overline{J} = \mathbb{V}(\mathfrak{q}) = \mathbb{V}(\mathfrak{p}) \subseteq J \subseteq \overline{J}$. This combines to $\mathbb{V}(\mathfrak{p}) = J$, which is the maximality of $\mathbb{V}(\mathfrak{p})$.

□

Proof of (8.94):

- Let us begin by proving that $I \mapsto \overline{I}$ is well-defined: As $I \subseteq U$ is non-empty, we have $\emptyset \neq I = I \cap U \subseteq \overline{I} \cap U$ and therefore $\overline{I} \cap U \neq \emptyset$. Also $\overline{I} \subseteq X$ is closed and (as I is irreducible) irreducible, by property (b) in (8.91.(i)).

 Next we will see, that $J \mapsto J \cap U$ is well-defined, too: $J \cap U \neq \emptyset$ is non-empty, by assumption. And as $J \subseteq X$ is closed, so is $J \cap U \subseteq U$ in the relative topology. It remains to prove, that $J \cap U$ is irreducible again: Consider any open non-empty subsets $P, Q \subseteq J \cap U$. That is $P = P' \cap (J \cap U)$ and $Q = Q' \cap (J \cap U)$ for some open subsets $P', Q' \subseteq X$. As $U \subseteq X$ is open, we see that P and Q are an open subset of J, e.g. for P we have

 $$P \;=\; P' \cap (J \cap U) \;=\; (P' \cap U) \cap J$$

 But as J is irreducible and P, Q are non-empty, open subsets of J we get $P \cap Q \neq \emptyset$. As this is true for any non-empty, open subsets of $J \cap U$, this means $J \cap U$ is irreducible again.

- The next step is proving that these maps are mutually inverse: We begin by arguing for $\overline{I} \cap U = I$: As $I \subseteq U$ the inclusion $I \subseteq \overline{I} \cap U$ is clear. Conversely, as $I \subseteq U$ is closed, it is of the form $I = I' \cap U$ for some $I' \subseteq X$ closed. As $I \subseteq I'$ we have $\overline{I} \subseteq I'$ and thereby $\overline{I} \cap U \subseteq I' \cap U = I$.

Now for $\overline{J \cap U} = J$, but this is easy: As $J \cap U \subseteq J$ is non-empty and open and J is irreducible, $J \cap U$ is dense in J, by property (c) of (8.90.(i)) and this already is $\overline{J \cap U} = J$.

- The correspondence of the irreducible components is straightforward: If we start with $I \in \mathrm{IRR}(U)$, then we have to show, that $\overline{I} \in \mathrm{IRR}(X)$. So suppose $\overline{I} \subseteq J$, then $I = \overline{I} \cap U \subseteq J \cap U$ and thereby $I = J \cap U$, as I is maximal. Then again $\overline{I} = \overline{J \cap U} = J$, which is the maximality of $\overline{I}$.

 Conversely, for $J \in \mathrm{IRR}(X)$ we have to show $J \cap U \in \mathrm{IRR}(U)$. Hence we consider $J \cap U \subseteq I$ for some irreducible $I \subseteq U$. Then $J = \overline{J \cap U} \subseteq \overline{I}$ and thereby $J = \overline{I}$, as J is maximal. Then again $J \cap U = \overline{I} \cap U = I$, which is the maximality of $J \cap U$.

- It remains to show the correspondence of generic points: For any $x \in U$ let us denote the closure of $\{ x \}$ in U by $I_x := \mathrm{cl}_U(\{ x \})$ and the closure in X by $J_x := \mathrm{cl}_X(\{ x \})$. Then by (6.16.(x)) we have $I_x = J_x \cap U$. So if we start with $J \cap U = I_x$, then I_x corresponds to J_x and thereby $J = J_x$. Conversely, if we start with $J = J_x$ we still have to prove $x \in U$. Suppose we had $x \notin U$, then $x \in J \setminus U$ which is a closed subset of J. In particular $J = J_x \subseteq J \setminus U$ and thereby $J \cap U = \emptyset$, which was assumed to be not the case. So we have $x \in U$ and thereby $J \cap U = J_x \cap U = I_x$ again.

□

Proof of (8.96):

(i) Let us first consider the case of a closed subset $C \subseteq X$: If $I_0 \subset \ldots \subset I_d \subseteq C$ is any chain of closed, irreducible subsets of C, then as $C \subseteq X$ is closed, any $I_k \subseteq C$ also is a closed subset $C \subseteq X$. Thus $I_0 \subset \ldots \subset I_d \subseteq X$ also is a chain of closed, irreducible subsets of X and therefore $\mathrm{tdim}(C) \leq \mathrm{tdim}(X)$.

(i) Let us now consider the case of an open subset $U \subseteq X$: If $I_0 \subset \ldots \subset I_d \subseteq C$ is any chain of closed, irreducible subsets of U, then by (8.94) this corresponds to a chain $\overline{I}_0 \subseteq \ldots \subseteq \overline{I}_d \subseteq X$ of closed, irreducible subsets of X. Suppose there was some $k \in 1 \ldots d$ such that $\overline{I}_{k-1} = \overline{I}_k$, then we had $I_{k-1} = \overline{I}_{k-1} \cap U = \overline{I}_k \cap U = I_k$, which is false. Thus $\overline{I}_0 \subset \ldots \subset \overline{I}_d \subseteq X$ is strictly increasing and thereby $d \leq \mathrm{tdim}(X)$. As this is true for any chain in U, we conclude $\mathrm{tdim}(U) \leq \mathrm{tdim}(X)$.

(ii) Since X is finite-dimensional, so is C by (i). The we may consider $I_0 \subset \ldots \subset I_d \subseteq C$ with $d = \mathrm{tdim}(C)$. As $C \subset X$ and X is irreducible, this chain may be appended, to $I_0 \subset \ldots \subset I_d \subset X$ and hence $\mathrm{tdim}(X) \geq d + 1 > d = \mathrm{tdim}(C)$.

(iii) If $I \in \mathrm{IRR}(X)$ is an irreducible component, then $I \subseteq X$ is closed and hence $\mathrm{tdim}(I) \leq \mathrm{tdim}(X)$ due to (i). This proves the first estimate $m := \max\{ \mathrm{tdim}(I) \mid I \in \mathrm{IRR}(X) \} \leq d := \mathrm{tdim}(X)$. Conversely consider a chain of maximal length $I_0 \subset \ldots \subset I_d \subseteq X$ in X. Then I_d has to maximal and hence $I_d \in \mathrm{IRR}(X)$. Thus we also get $d \leq \mathrm{tdim}(I_d) \leq m$.

□

Proof of (8.97):

- (a) $\implies$ (d): Let $U := \bigcup_{i \in \mathbb{N}} U_i$. Then by assumption U admits a finite subcover, that is there is a finite set $\Omega \subseteq \mathbb{N}$ such that $U = \bigcup_{i \in \Omega} U_i$. Now let $n := \max(\Omega) \in \mathbb{N}$ be the maximal number contained in Ω, then for any $i \in \Omega$ we have $U_i \subseteq U_n$, as the U_i form an ascending chain. Hence for any $k \in \mathbb{N}$ we get the inclusions $U_{n+k} \subseteq U = \bigcup_{i \in \Omega} U_i = U_n \subseteq U_{n+k}$.

- (d) $\Longrightarrow$ (a): Consider $U = \bigcup_{i\in I} U_i$, if I is finite, then there is nothing to prove, thus we may assume I to be infinite. As $U_i \subseteq U$ and $U \subseteq X$ are open, $U_i \subseteq X$ is open, too. Now choose any $i(0) \in I$ and let $V_0 := U_{i(0)}$. Suppose we have already constructed $V_k \subseteq U$ and that $U \neq V_k$. Then there is some $x \in U \setminus V_k$ and hence some $i(k+1) \in I$ such that $x \in U_{i(k+1)}$. Now let $V_{k+1} := V_k \cup U_{i(k+1)} = U_{i(0)} \cup \cdots \cup U_{i(k)} \cup U_{i(k+1)}$. Then we found a strictly ascending chain

$$V_0 \subset \ldots \subset V_k \subset V_{k+1}$$

 Due to (d) this cannot rise indefinitely, which means that there has to be some index $n \in \mathbb{N}$ at which $U = V_n = U_{i(0)} \cup \cdots \cup U_{i(n)}$. That is we have found a finite subcover of U.

- (d) $\Longrightarrow$ (b): Let $\mathcal{U} := \{ U_i \mid i \in I \}$ for some index set I and suppose $\mathcal{U}$ had no maximal element. We begin with any $i(0) \in I$. Now suppose we have already chosen $i(0), \ldots, i(k) \in I$ in such a way that $U_{i(0)} \subset \ldots \subset U_{i(k)}$, then we continue: As $\mathcal{U}$ does not have a maximal element, $U_{i(k)}$ is not maximal and this means there is some $i(k+1) \in I$ such that $U_{i(k)} \subset U_{i(k+1)}$. That is we can always append the chain in such a way, that $U_{i(0)} \subset \ldots \subset U_{i(k)} \subset U_{i(k+1)}$. Thereby we obtain a strictly ascending chain of open sets, that does not become stationary, in contradiction to (d). This contradiction yields, that $\mathcal{U}$ *has* a maximal element.

- (b) $\Longrightarrow$ (d): Consider $\mathcal{U} := \{ U_i \mid i \in \mathbb{N} \}$, by assumption (b) $\mathcal{U}$ has a maximal element $U^* = U_n$ for some $n \in \mathbb{N}$. But for any $k \in \mathbb{N}$ we also have $U_n \subseteq U_{n+k}$ as the U_i form an ascending chain. Thus $U_n = U_{n+k}$ by maximality of U_n.

- Thus we have obtained the equivalences (a) $\Longleftrightarrow$ (b) $\Longleftrightarrow$ (d). But by going to complements the equivalences (b) $\Longleftrightarrow$ (c) and (d) $\Longleftrightarrow$ (e) are obvious.

□

Proof of (8.98):

(i) This is just a side-effect of the Laskar-Noether theorem, that will be proved right after this proposition (and not be used before, of course). The reader is asked to refer to (8.99).

(iv) Let us first assume that $L = C \subseteq X$ is a closed subset. If now $C_1 \supseteq C_2 \supseteq \ldots$ is a descending chain of closed subsets $C_i \subseteq C$, then clearly $C_i \subseteq X$ is closed, too. And as X was assumed to be noetherian the chain has to stabilize, which proves, that C is noetherian, too.

(iii) Let $L = C \cap U$, where $C \subseteq X$ is closed and $U \subseteq X$ is open, we will prove, that L is compact. To do this consider any cover $L = \bigcup_i U_i$ (where $i \in I$) by open sets $U_i \subseteq L$. By definition of the relative topology there are open subsets $U_i' \subseteq X$ such that $U_i = U_i' \cap L$. And if we let $V_i := U \cap U_i'$, then $V_i \subseteq X$ is open and we get $U_i = U_i' \cap L = C \cap V_i$. Hence we have

$$C \cap U = L = \bigcup_{i\in I} U_i = \bigcup_{i\in I} C \cap V_i$$

That is the open subset $C \cap U \subseteq C$ is covered by the open sets $C \cap V_i \subseteq C$. But (iv) above (for closed sets) C is noetherian and hence $C \cap U$ is compact, by property (a) of (8.97). That is there

is some finite subset $\Omega \subseteq I$ such that

$$L \;=\; C \cap U \;=\; \bigcup_{i\in\Omega} C \cap V_i \;=\; \bigcup_{i\in\Omega} U_i$$

(iv) Let us now prove the claim for general locally closed subsets $L \subseteq X$, say $L = C \cap U$ again. Consider an open subset $K \subseteq L$, that is $K = V \cap L$ for some $V \subseteq X$ open and hence we find, that $K = V \cap L = C \cap (U \cap V)$ is a locally closed subset $K \subseteq X$ again. Thus it is compact, due to (iii) above. That is any open subset of L is compact, which means that L satisfies property (a) of (8.97) and hence is a noetherian topological space.

(v) Consider the set $\mathcal{F} := \{\, C \subseteq X \text{ closed} \mid \varphi(C) = \text{ false} \,\}$. If $\mathcal{F} \neq \emptyset$ then $\mathcal{F}$ has a minimal element $F \in \mathcal{F}$, since X is noetherian. As $\varphi(\emptyset)$ is true, we have $F \neq \emptyset$. And if $C \subseteq X$ is closed with $C \subset F$, then $\varphi(C)$ has to be true, by the minimality of F. Thus by assumption we also get $\varphi(F) = $ true, a contradiction. Therefore $\mathcal{F} = \emptyset$ and this means $\varphi(C)$ is true for any closed subset $C \subseteq X$, in particular for $C = X$.

□

Proof of (8.99):
Existence: Let us denote $\mathcal{E} := \{\, X \subseteq N \text{ closed} \mid \text{existence not satisfied} \,\}$. That is $\mathcal{E}$ is a collection of closed subsets of N. If $\mathcal{E}$ was non-empty, then there was a minimal subset $X \in \mathcal{E}$ (as N is noetherian). In particular X is reducible (else the existence was satisfied trivially). That is $X = C \cup D$ for some closed subsets $C, D \subseteq X$ with $C, D \neq X$. As X has been minimal we get $C, D \notin \mathcal{E}$. Yet C and D are closed in X and hence in N, which means that C and D have to allow the existence. That is

$$\begin{aligned} C &= C_1 \cup \cdots \cup C_r \\ D &= D_1 \cup \cdots \cup D_s \end{aligned}$$

From this we get $X = C \cup D = C_1 \cup \cdots \cup C_r \cup D_1 \cup \cdots \cup D_s$. In this representation the properties (1), (3) and (4) are satisfied trivially. And by scratching the redundant C_i and D_j we may also guarantee property (2). Thus X also allows the existence and hence $X \notin \mathcal{E}$, a contradiction. This only leaves $\mathcal{E} = \emptyset$, that is any closed subset X of N allows a decomposition satisfying (1) to (4).

Uniqueness: Suppose $X_1 \cup \cdots \cup X_r = X = Y_1 \cup \cdots \cup Y_s$ such that the X_i and Y_i satisfy the properties (1) to (3). As $X_i \subseteq X$ we have $X_i = X_i \cap X$ and as $X = \bigcup_j Y_j$ this implies

$$X_i \;=\; \bigcup_{j=1}^{s} X_i \cap Y_j$$

As Y_j is closed in X it is closed in N and hence $X_i \cap Y_j$ is closed in X_i. As X_i is irreducible this implies that there is some $j \in 1 \ldots s$ such that $X_i = X_i \cap Y_j$. That is $X_i \subseteq Y_j$. In complete analogy to the above we find some $k \in 1 \ldots r$ such that $Y_j \subseteq X_k$. Hence $X_i \subseteq Y_j \subseteq X_k$. By property (2) this implies $i = k$ and hence $X_i = Y_j$. Now let $\sigma(i) := j$ and use this construction for any $i \in 1 \ldots r$, then $\sigma : 1 \ldots r \to 1 \ldots s$ is a mapping. And if $\sigma(i) = \sigma(j)$ then $X_i = Y_{\sigma(i)} = Y_{\sigma(j)} = X_j$ such that $i = j$ due to property (2). That is σ is injective and hence $r \leq s$. Exchanging the roles of the X_i and Y_j we also find

$s \leq r$ and hence $r = s$. That is σ is a permutation and this is the uniqueness.

Property (5): As N is a noetherian topological space, so is X, according to (8.98.(iv)). And hence X has only finitely many irreducible components, as we have seen in (8.98.(i)). Now let $\mathcal{I} := \{ X_1, \ldots, X_r \}$ and take a look at the second part of (8.93). Property (1) there is property (1) here. Property (2) there are properties (3) and (4) here and we also get property (3) there: For ease of notation we prove $X \neq X_2 \cup \cdots \cup X_r$ only: Suppose $X_1 \subseteq X = X_2 \cup \cdots \cup X_r$, as X_1 is irreducible and any X_i (for $i \in 2 \ldots r$) is closed we have $X_1 \subseteq X_k$ for some $k \in 2 \ldots r$, which is forbidden by property (2) here. Thus we also have property (3) of (8.93) and conclude $\mathcal{I} = \operatorname{IRR}(X)$. □

Proof of (8.100):
Let us first assume that $X = \{ x_1, \ldots, x_r \}$ is finite and denote $X_i := \{ x_i \}$, then we have to show that $\operatorname{tdim}(X) = 0$. It is clear that any X_i is irreducible and as X is T_1 the $X_i \subseteq X$ are closed, too. And by construction we also have $X = X_1 \cup \cdots \cup X_r$ and $X_i \not\subseteq X_j$ for any $i \neq j \in 1 \ldots r$. Altogether the X_i satisfy properties (1) to (4) in (8.99) and hence we get $\operatorname{IRR}(X) = \{ X_1, \ldots, X_r \}$. Now suppose that $I_0 \subset I_1 \subset \ldots \subset I_d$ is a chain of closed, irreducible subsets of X, such that I_0 is non-empty. As $I_0 \neq \emptyset$ there is some $x_i \in I_0$ and hence $X_i \subseteq I_k$ (for any $k \in 0 \ldots d$). As X_i is maximal (an irreducible component) we get $X_i = I_0 = I_1 = \cdots = I_d$ and hence $d = 0$. In particular $\operatorname{tdim}(X) = 0$ which had to be shown.
Conversely assume that $\operatorname{tdim}(X) = 0$, then we need to show that X is finite. Thus consider any point $x \in X$ and any irreducible set $I \subseteq X$ with $\{ x \} \subseteq I$. As I is irreducible, so is $\overline{I}$, due to (8.91.(i)). And as X has been assumed to T_1 we know that $\{ x \} \subseteq X$ is closed, such that $\{ x \} \subseteq \overline{I}$ is a chain of closed, irreducible subsets. Yet as $\operatorname{tdim}(X) = 0$ this implies $I \subseteq \overline{I} = \{ x \} \subseteq I$ and hence $I = \{ x \}$. That is $\{ x \}$ is maximal, in other words an irreducible component of X. But by (8.98.(i)) X only has finitely many irreducible components. In particular we get $\#X = \#\operatorname{IRR}(X) < \infty$ as claimed. □

Proof of (8.103):
If $X = \emptyset$, there is nothing to prove, as $\operatorname{IRR}(X) = \{ \emptyset \} = \operatorname{CNC}(X)$. Thus assume $X \neq \emptyset$ and let us denote the irreducible components by $\operatorname{IRR}(X) = \{ I_1, \ldots, I_s \}$, thereby s is finite, due to (8.98.(i)). Any irreducible subset $I \subseteq X$ already is connected by (8.91.(iii)). And as any $I_j \neq \emptyset$ is non-empty and connected proposition (6.37.(ii)) implies that there is a uniquely determined connected component $K \in \operatorname{CNC}(X)$ such that $I_j \subseteq K$. Thus let $\{ K_1, \ldots, K_r \} \subseteq \operatorname{CNC}(X)$ be a collection of connected components of X such that

$$\forall\, j \in 1 \ldots s \;\; \exists\, i \in 1 \ldots r \;\; : \;\; I_j \subseteq K_i$$

By removing duplicates, we can take the K_i to be are pairwise distinct, that is $K_h = K_i$ implies $i = h$. For any $i \in 1 \ldots r$ let us now denote $J(i) := \{ j \in 1 \ldots s \mid I_j \subseteq K_i \}$. Suppose we had $j \in J(h) \cap J(i)$ then $I_j \subseteq K_h \cap K_i$. However, by construction, distinct connected components are disjoint and as $I_j \neq \emptyset$ we hence conclude $K_h = K_i$. As we have taken the K_i to be pairwise distinct, this implies $h = i$. That is the $J(i)$ are pairwise disjoint and hence we have partitioned $1 \ldots s$ into $(1 \ldots s) = J(1) \cup \cdots \cup J(r)$. Altogether we have

$$X \;=\; \bigcup_{j=1}^{s} I_j \;=\; \bigcup_{i=1}^{r} \bigcup_{j \in J(i)} I_j \;\subseteq\; \bigcup_{i=1}^{r} K_i \;\subseteq\; X$$

That is $X = \bigcup_i K_i$. Now consider any *any* connected component $L \in \operatorname{CNC}(X)$. As $L \neq \emptyset$ (by maximality)

we may choose some $x \in L \subseteq X$. Thus there is some $i \in 1 \dots r$ such that $x \in K_i$. For this i we get $L \cap K_i \neq \emptyset$. And as distinct connected components would be disjoint, this implies $L = K_i$. Thus we have also obtained $\mathrm{CNC}(X) \subseteq \{ K_1 \dots, K_r \}$. By construction the map $(1 \dots s) \twoheadrightarrow (1 \dots r) : j \mapsto i$ such that $I_j \subseteq K_i$ is surjective and hence

$$\#\mathrm{CNC}(X) \;=\; r \;\leq\; s \;=\; \#\mathrm{IRR}(X)$$

In particular X has only finitely may connected components and hence (6.37.(iv)) yields a partition of X into the topological sum $X = K_1 \oplus \dots \oplus K_r$. In particular any K_i is both, open and closed. Next we will prove the following implication for any $j \in 1 \dots s$ and any $i \in 1 \dots r$

$$I_j \cap K_i \neq \emptyset \quad\Longrightarrow\quad I_j \subseteq K_i$$

First of all $I_j \cap K_i \subseteq I_j$ is open and closed, as $K_i \subseteq X$ is open and closed. But as I_j is irreducible any non-empty open subset is dense, in particular $I_j \cap K_i \subseteq I_j$ is dense. But as $I_j \subseteq K_i \subseteq I_j$ also is closed we get $I_j \cap K_i = I_j$, which translates into $I_j \subseteq K_i$. As $(1 \dots s) = I(1) \cup \dots \cup I(r)$ and $I(j) = \mathcal{I}(K_j)$ by construction this translates into the the first identity of $\mathrm{IRR}(X)$ in the claim. It remains to verify that the second identity for K, which reads as (for any $i \in 1 \dots r$)

$$K_i \;=\; \bigcup_{j \in J(i)} I_j$$

By definition of $J(i)$ we have $I_j \subseteq K_i$ for any $j \in J(i)$. And this implies " $\supseteq$ ". Conversely consider any $x \in K_i \subseteq X = I_1 \cup \dots \cup I_s$, then there is some $j \in 1 \dots s$ such that $x \in I_j$. For this j we now have $x \in I_j \cap K_i$ and hence $I_j \subseteq K_i$ by the above implication. Thus we have found $x \in I_j$ for some $j \in J(i)$ and as this is true for any $x \in K_i$, this also grants the inclusion " $\subseteq$ ". □

Proof of (8.104):
We start with (a) $\Longrightarrow$ (b), that is $\mathfrak{m} = Rm_1 + \dots + Rm_n$ is generated as an R-module. Then it is clear that $\{m_i + \mathfrak{m}^2 \mid i \in 1 \dots n\}$ is a generating set of $\mathfrak{m}/\mathfrak{m}^2$: Given any $x + \mathfrak{m}^2 \in \mathfrak{m}/\mathfrak{m}^2$ we may choose $a_1, \dots, a_n \in R$ such that $x = a_1 m_1 + \dots + a_n m_n$ and thereby $x + \mathfrak{m}^2 = \sum_i a_i m_i + \mathfrak{m}^2 = \sum_i (a_i + \mathfrak{m})(m_i + \mathfrak{m}^2)$. As R is noetherian $\mathfrak{m}$ is finitely generated. Hence we may choose a generating set with a minimal number generators and for this we find

$$\dim_E \left(\mathfrak{m} \Big/ \mathfrak{m}^2 \right) \;\leq\; \#\left\{ m_i + \mathfrak{m}^2 \mid i \in 1 \dots n \right\} \;\leq\; n \;=\; \mathrm{rank}_R(\mathfrak{m})$$

Conversely for (b) $\Longrightarrow$ (a), we start with a set $\{m_i + \mathfrak{m}^2 \mid i \in 1 \dots n\}$ that generates $\mathfrak{m}/\mathfrak{m}^2$ as an E-vector-space. Then we let $\mathfrak{a} := Rm_1 + \dots + Rm_n \trianglelefteq_{\mathfrak{i}} R$. We will now prove, that

$$\mathfrak{m} \;=\; \mathfrak{a} + \mathfrak{m}^2$$

As any $m_i \in \mathfrak{m}$ we also have $\mathfrak{a} \subseteq \mathfrak{m}$ and $\mathfrak{m}^2 \subseteq \mathfrak{m}$ is clear such that $\mathfrak{a} + \mathfrak{m}^2 \subseteq \mathfrak{m}$ and we have the inclusion " $\supseteq$ ". Conversely if we are given any $x \in \mathfrak{m}$ then we may choose $a_i + \mathfrak{m} \in E$ such that $x + \mathfrak{m}^2 = \sum_i (a_i + \mathfrak{m})(m_i + \mathfrak{m}^2) = (\sum_i a_i m_i) + \mathfrak{m}^2$. Hence we have $d := x - \sum_i a_i m_i \in \mathfrak{m}^2$. Thereby $a := \sum_i a_i m_i \in \mathfrak{a}$ by construction, such that $x = a + d \in \mathfrak{a} + \mathfrak{m}^2$. This is the converse inclusion " $\subseteq$ "
Now remark that $\mathrm{JAC}(R) = \mathfrak{m}$, as R is a local ring. Furthermore we have $\mathfrak{m}^2 = \mathfrak{m}\,\mathfrak{m}$ and $\mathfrak{m}$ is a

finitely generated R-module, as R is noetherian. Thus by the lemma of Nakayama (3.44.(iii)) [using the parameters $P := \mathfrak{a}$, $M := \mathfrak{m}$ and $\mathfrak{a} := \mathfrak{m}$] we find $\mathfrak{m} = \mathfrak{a}$. That is $\{ m_1, \ldots, m_n \}$ generates $\mathfrak{m}$. If we start with a basis $m_i + \mathfrak{m}^2$ of $\mathfrak{m}/\mathfrak{m}^2$ we in particular find, that

$$\operatorname{rank}_R(\mathfrak{m}) \;\leq\; n \;=\; \dim_E \left(\mathfrak{m} \Big/ \mathfrak{m}^2 \right)$$

□

Proof of (8.106):
If $\mathfrak{p} = \mathfrak{m}$, then $\operatorname{height}(\mathfrak{p}) = \operatorname{height}(\mathfrak{m})$ is clear. Conversely suppose $\operatorname{height}(\mathfrak{p}) = \operatorname{height}(\mathfrak{m})$ and pick up a CPI $(\mathfrak{p}_0, \ldots, \mathfrak{p}_r)$ of R, with $\mathfrak{p}_r = \mathfrak{p}$ and $r = \operatorname{height}(\mathfrak{p})$. Now $\mathfrak{p}_r$ is contained in a maximal ideal by (2.4.(ii)). And as R is local there is only one maximal ideal around: $\mathfrak{p}_r \subseteq \mathfrak{m}$. Suppose we had $\mathfrak{p}_r \subset \mathfrak{m}$, then $(\mathfrak{p}_0, \ldots, \mathfrak{p}_r, \mathfrak{m})$ would be a CPI, too and hence $\operatorname{height}(\mathfrak{m}) \geq r+1$, in contradiction to $\operatorname{height}(\mathfrak{m}) = r$. Thus we have the identity $\mathfrak{p} = \mathfrak{p}_r = \mathfrak{m}$, as claimed. □

Proof of (8.107):
Clearly for any ideal $\mathfrak{m}$ of R we have $\operatorname{height}(\mathfrak{m}) \leq \operatorname{kdim}(R)$. Conversely consider $(\mathfrak{p}_0, \ldots, \mathfrak{p}_d)$ any CPI of R. If $\mathfrak{p}_d$ is not maximal itself, then it is contained in a maximal ideal by (2.4.(ii)) and we may append this chain. Therefore we may assume $\mathfrak{p}_d$ to be a maximal ideal. As R is a local ring there is one choice only: $\mathfrak{p}_d = \mathfrak{m}$. Therefore $d \leq \operatorname{height}(\mathfrak{m})$ and as this is true for any CPI, we conclude $\operatorname{kdim}(R) \leq \operatorname{height}(\mathfrak{m})$, too. That is $\operatorname{kdim}(R) = \operatorname{height}(\mathfrak{m})$ and by Krull's height theorem (8.80.(iii)) - recall that R also is assumed to be noetherian - we have $\operatorname{height}(\mathfrak{m}) < \operatorname{rank}(\mathfrak{m}) < \infty$.

Let n be the minimal number of elements $a_1, \ldots, a_n \in R$ such that $\mathfrak{m}$ is a minimal prime ideal over $\mathfrak{a} := \langle a_1, \ldots, a_n \rangle_{\mathfrak{i}}$. Then by Krull's height theorem (8.80.(ii)) we have $\operatorname{height}(\mathfrak{m}) \leq n$ and thereby $\operatorname{kdim}(R) \leq n$. Conversely if $d = \operatorname{kdim}(R) = \operatorname{height}(\mathfrak{m})$ then by the reverse direction in (8.80.(ii)) there are some $a_1, \ldots, a_d \in R$ such that $\mathfrak{m}$ is a minimal prime ideal over $\langle a_1, \ldots, a_d \rangle_{\mathfrak{i}}$. As n is the minimal number for which this is possible we also have $n \leq d = \operatorname{kdim}(R)$. □

Proof of (8.109):

(i) Let us abbreviate $\overline{R} := R/\mathfrak{a}$ and for any $b \in R$ also $\overline{b} := b + \mathfrak{a}$. As R is noetherian, so is $\overline{R}$, as any chain of ideals in $\overline{R}$ originates from a chain of ideals in R. Also R is a local ring with maximal ideal $\overline{\mathfrak{m}} := \mathfrak{m}/\mathfrak{a}$ by the correspondence theorem (1.71). Let $n := \operatorname{kdim}(\overline{R})$, which is finite, by (8.107). Then we may pick up a local system of parameters $\left\{ \overline{b}_1, \ldots, \overline{b}_n \right\}$ of $\overline{R}$. That is $\overline{\mathfrak{m}}$ is a prime ideal, minimal over $\overline{\mathfrak{b}} := \langle \overline{b}_1, \ldots, \overline{b}_n \rangle_{\mathfrak{i}}$. We will prove that $\mathfrak{m}$ is a minimal prime ideal over $\mathfrak{a} + \mathfrak{b}$, as well: To do this consider any prime ideal $\mathfrak{p} \in \operatorname{Spec}(R)$ in between $\mathfrak{a} + \mathfrak{b} \subseteq \mathfrak{p} \subseteq \mathfrak{m}$. By going to quotients $/\mathfrak{a}$ this chain turns into

$$\overline{\mathfrak{b}} \;=\; \langle \overline{b}_1, \ldots, \overline{b}_n \rangle_{\mathfrak{i}} \;=\; \mathfrak{a} + \mathfrak{b} \Big/ \mathfrak{a} \;\subseteq\; \mathfrak{p} \Big/ \mathfrak{a} \;\subseteq\; \mathfrak{m} \Big/ \mathfrak{a} \;=\; \overline{\mathfrak{m}}$$

But $\overline{\mathfrak{m}}$ is a minimal prime ideal over $\overline{\mathfrak{b}}$ such that we get $\overline{\mathfrak{p}} = \overline{\mathfrak{m}}$ and from this we get $\mathfrak{p} = \mathfrak{m}$ by correspondence (as $\mathfrak{a} \subseteq \mathfrak{p}$, as well). Thus $\mathfrak{m}$ is a minimal prime ideal over $\mathfrak{a} + \mathfrak{b}$ and therefore Krull's height theorem (8.80.(ii)) tells us $\operatorname{kdim}(R) = \operatorname{height}(\mathfrak{m}) \leq m + n = m + \operatorname{kdim}(\overline{R})$. In other words, we have found the claim $\operatorname{kdim}(R) - m \leq \operatorname{kdim}(\overline{R})$.

(ii) Let $\mathfrak{b} := \langle a_{m+1}, \ldots, a_n \rangle_{\mathfrak{i}}$, that is $\mathfrak{a} + \mathfrak{b} = \langle a_1, \ldots, a_n \rangle_{\mathfrak{i}}$. Then by assumption we have $n = \operatorname{kdim}(R)$

and $\mathfrak{m}$ is a prime ideal, minimal over $\mathfrak{a}+\mathfrak{b}$. As in the proof of (i) let us abbreviate $\overline{R} := R/\mathfrak{a}$, $\overline{a}_i := a_i + \mathfrak{a}_i$ and $\overline{\mathfrak{m}} := \mathfrak{m}/\mathfrak{a}$. Then the residue of $\mathfrak{a}+\mathfrak{b}$ in $\overline{R}$ is $\overline{\mathfrak{b}} = \langle \overline{a}_{m+1}, \ldots, \overline{a}_n \rangle_{\mathfrak{i}}$. Let us now prove, that $\overline{\mathfrak{m}}$ is a prime ideal minimal over $\overline{\mathfrak{b}}$. That is we consider any prime ideal $\overline{\mathfrak{p}}$ in between $\overline{\mathfrak{b}} \subseteq \overline{\mathfrak{p}} \subseteq \overline{\mathfrak{m}}$. That is $\overline{\mathfrak{p}} = \mathfrak{p}/\mathfrak{a}$ for some $\mathfrak{p} \in \operatorname{Spec}(R)$ with $\mathfrak{a} \subseteq \mathfrak{p}$. By assumption we have $a_k \in \mathfrak{p}$ for any $k \in m+1 \ldots n$ and therefore $\mathfrak{b} \subseteq \mathfrak{p}$. Together this is $\mathfrak{a}+\mathfrak{b} \subseteq \mathfrak{p} \subseteq \mathfrak{m}$ and thereby $\mathfrak{p} = \mathfrak{m}$, as $\mathfrak{m}$ is a prime ideal minimal over $\mathfrak{a}+\mathfrak{b}$. But from this we find $\overline{\mathfrak{p}} = \overline{\mathfrak{m}}$ and hence $\overline{\mathfrak{m}}$ is a prime ideal of $\overline{R}$, minimal over $\overline{\mathfrak{b}}$.

(iii) Suppose $\operatorname{kdim}(R/\mathfrak{a}) = \operatorname{kdim}(R) - m$ and let $n := \operatorname{kdim}(R)$. As $\overline{R} := R/\mathfrak{a}$ is a noetherian, local ring by (i), we find a local system of parameters $\left\{ \overline{b}_1, \ldots, \overline{b}_s \right\}$ of $\overline{R}$. In particular $\overline{\mathfrak{m}} = \mathfrak{m}/\mathfrak{a}$ is a prime ideal minimal over $\overline{\mathfrak{b}} := \langle \overline{b}_1, \ldots, \overline{b}_s \rangle_{\mathfrak{i}}$ and we have $s = \operatorname{kdim}(\overline{R}) = n - m$. Therefore $\{ a_1, \ldots, a_m, b_1, \ldots, b_s \}$ contains $n = \operatorname{kdim}(R)$ many elements. Now let $\mathfrak{b} := \langle b_1, \ldots, b_s \rangle_{\mathfrak{i}}$ and consider any prime ideal $\mathfrak{p} \in \operatorname{Spec}(R)$ such that $\mathfrak{a}+\mathfrak{b} \subseteq \mathfrak{p} \subseteq \mathfrak{m}$. As in (i) above we find $\overline{\mathfrak{p}} \subseteq \overline{\mathfrak{m}}$ and hence $\mathfrak{p} = \mathfrak{m}$, as $\mathfrak{a} \subseteq \mathfrak{p}$, too. Thus $\mathfrak{m}$ is a prime ideal minimal over $\mathfrak{a}+\mathfrak{b} = \langle a_1, \ldots, a_m, b_1, \ldots, b_s \rangle_{\mathfrak{i}}$ and therefore $\{ a_1, \ldots, a_m, b_1, \ldots, b_s \}$ is a local set of parameters of R. That is we have been able to append $\{ a_1, \ldots, a_m \}$.

(iii) Suppose we can append $\{ a_1, \ldots, a_m \}$ to a local system of parameters, $\{ a_1, \ldots, a_n \}$ of R, then by (ii) $\mathfrak{m}/\mathfrak{a}$ is a prime ideal minimal over $\langle a_{m+1}, \ldots, a_n \rangle_{\mathfrak{i}}$. Hence by Krull's height theorem (8.80.(ii)) we have $\operatorname{height}(\mathfrak{m}/\mathfrak{a}) \leq n - m$. But this is

$$\operatorname{kdim}\left(R \Big/ \mathfrak{a}\right) \;=\; \operatorname{height}\left(\mathfrak{m} \Big/ \mathfrak{a}\right) \;\leq\; n - m \;=\; \operatorname{kdim}(R) - m$$

But we also have $\operatorname{kdim}(R/\mathfrak{a}) \geq \operatorname{kdim}(R) - m$ by (i), so together this can be combined to the equality $\operatorname{kdim}(R/\mathfrak{a}) \geq \operatorname{kdim}(R) - m$.

(iv) We use theorem (8.80.(v)): As $m = \operatorname{height}(\mathfrak{a}) \leq \operatorname{kdim}(R) = \operatorname{height}(\mathfrak{m}) =: n$ we can append elements $a_{m+1}, \ldots, a_n \in \mathfrak{m}$ such that for any $k \in m \ldots n$ we get: Let $\mathfrak{a}_k := \langle a_1, \ldots, a_k \rangle_{\mathfrak{i}}$ and $\mathfrak{p}_k$ be a prime ideal minimal over $\mathfrak{a}_k$, then we get $\operatorname{height}(\mathfrak{p}_k) = k$. In particular $\operatorname{height}(\mathfrak{p}_n) = n = \operatorname{height}(\mathfrak{m})$. But $\mathfrak{m}$ is the one and only ideal in R of height n, by (8.106), such that we conclude $\mathfrak{p}_n = \mathfrak{m}$. That is $\mathfrak{m}$ is a prime ideal, minimal over $\langle a_1, \ldots, a_n \rangle_{\mathfrak{i}}$ and $n = \operatorname{height}(\mathfrak{m}) = \operatorname{kdim}(R)$. In other words $\{ a_1, \ldots, a_n \}$ is a system of local parameters of R - we have been able, to append $\{ a_1, \ldots, a_m \}$, which is part (1) of the claim. Now by (iii) we have $\operatorname{kdim}(R/\mathfrak{a}) = \operatorname{kdim}(R) - m = \operatorname{kdim}(R) - \operatorname{height}(\mathfrak{a})$, which already is (3). Also we know by (ii), that $\mathfrak{m}/\mathfrak{a}$ is a prime ideal, minimal over $\langle a_{m+1} + \mathfrak{a}, \ldots, a_n + \mathfrak{a} \rangle_{\mathfrak{i}}$. But by (3) we have just seen $\operatorname{kdim}(R/\mathfrak{a}) = \operatorname{kdim}(R) - m = n - m$, which makes $\{ a_{m+1} + \mathfrak{a}, \ldots, a_n + \mathfrak{a} \}$ a local system of parameters for $R/\mathfrak{a}$.

□

15.10 Proofs of Chapter 11

Proof of (11.10):

(ii) We start with (b) $\Longrightarrow$ (a): Choose $T := X$, then $\varphi^* : \mathcal{C}(Y,X) \twoheadrightarrow \mathcal{C}(X,X)$ is surjective, by assumption. As $\mathbb{1}_X \in \mathcal{C}(X,X)$ there is some $\overline{\varphi} \in \mathcal{C}(Y,X)$ such that $\overline{\varphi} \circ \varphi = \varphi^*(\overline{\varphi}) = \mathbb{1}_X$ and this is (a). Conversely suppose (a), that is $\overline{\varphi} \circ \varphi = \mathbb{1}_X$. Then we regard the chain

$$\mathcal{C}(X,T) \xrightarrow{\overline{\varphi}^*} \mathcal{C}(Y,T) \xrightarrow{\varphi^*} \mathcal{C}(X,T)$$

Starting with any $\tau \in \mathcal{C}(X,T)$, this is mapped to $\tau \mapsto \overline{\varphi}^*(\tau) = \tau \circ \overline{\varphi}$ which in turn is mapped to $\overline{\varphi}^*(\tau) \mapsto \varphi^*(\tau \circ \overline{\varphi}^*) = (\tau \circ \overline{\varphi}) \circ \varphi = \tau \circ (\overline{\varphi} \circ \varphi) = \tau \circ \mathbb{1}_X = \tau$. That is $\varphi^*\overline{\varphi}^*$ is the identity map on $\mathcal{C}(X,T)$ and thereby we see that φ^* is surjective (and $\overline{\varphi}^*$ is injective).

(iv) We start with (b) $\Longrightarrow$ (a) again: Choose $T := Y$, then $\varphi_* : \mathcal{C}(Y,X) \twoheadrightarrow \mathcal{C}(Y,Y)$ is surjective, by assumption. As $\mathbb{1}_Y \in \mathcal{C}(Y,Y)$ there is some $\overline{\varphi} \in \mathcal{C}(Y,X)$ such that $\varphi \circ \overline{\varphi} = \varphi_*(\overline{\varphi}) = \mathbb{1}_Y$ and this is (a). Conversely suppose (a), that is $\varphi \circ \overline{\varphi} = \mathbb{1}_Y$. Then we regard the chain

$$\mathcal{C}(T,Y) \xrightarrow{\overline{\varphi}_*} \mathcal{C}(T,X) \xrightarrow{\varphi_*} \mathcal{C}(T,Y)$$

Starting with any $\tau \in \mathcal{C}(T,Y)$, this is mapped to $\tau \mapsto \overline{\varphi}_*(\tau) = \overline{\varphi} \circ \tau$ which in turn is mapped to $\overline{\varphi}_*(\tau) \mapsto \varphi_*(\overline{\varphi}^* \circ \tau) = \varphi \circ (\overline{\varphi} \circ \tau) = (\varphi \circ \overline{\varphi}) \circ \tau = \mathbb{1}_Y \circ \tau = \tau$. That is $\varphi_*\overline{\varphi}_*$ is the identity map on $\mathcal{C}(T,Y)$ and thereby we see that φ_* is surjective (and $\overline{\varphi}_*$ is injective).

(v) We begin with the equivalence of (c) and (d): The implication (d) $\Longrightarrow$ (c) is trivial, by taking $\psi_X := \psi$ and $\psi_Y := \psi$. Conversely let us prove that $\psi_X = \psi_Y$ in (c): To do this compute:

$$\psi_X \;=\; \psi_X \circ \mathbb{1}_Y \;=\; \psi_X \circ \big(\varphi \circ \psi_Y\big) \;=\; \big(\psi_X \circ \varphi\big) \circ \psi_Y \;=\; \mathbb{1}_X \circ \psi_Y \;=\; \psi_Y$$

Thereby we see that $\psi := \varphi_X = \psi_Y$ is the inverse of φ. We need to prove that this ψ is uniquely determined. So let us suppose we have ψ_1 and ψ_2 that both are inverses of φ. Then we need to show $\psi_1 = \psi_2$. But this can be done in the same manner as before:

$$\psi_1 \;=\; \psi_1 \circ \mathbb{1}_Y \;=\; \psi_1 \circ \big(\varphi \circ \psi_2\big) \;=\; \big(\psi_1 \circ \varphi\big) \circ \psi_2 \;=\; \mathbb{1}_X \circ \psi_2 \;=\; \psi_2$$

Also (a) is equivalent to (e): By (iv) φ is an split-epimorphsim, if and only if φ_* is surjective, for any object T. And φ is a monomorphism, if and only if φ_* is injective, for any object T. Together this is φ_* is bijective, for any object T.

Likewise (b) is equivalent of (f): By (ii) φ is a split-monomorphism, if and only if φ^* is surjective, for any object T. And φ is an epimorphism, if and only if φ^* is injective, for any object T. Together this is φ^* is bijective, for any object T.

Let us now prove the equivalence of (a) and (d): Suppose (a), as φ is a split-monomorphism, there is some $\psi \in \mathcal{C}(Y,X)$, such that $\psi \circ \varphi = \mathbb{1}_X$. Now compute $(\varphi \circ \psi) \circ \varphi = \varphi \circ (\psi \circ \varphi) = \varphi \circ \mathbb{1}_X = \varphi = \mathbb{1}_Y \circ \varphi$. As φ also is an epimorphism, we can conclude $\varphi \circ \psi = \mathbb{1}_Y$ and thereby have (d). And from (d) we immediately get (e): An inverse map of $\varphi^* : \tau \mapsto \tau \circ \varphi$ is obviously given by $(\varphi^{-1})^* : \vartheta \mapsto \vartheta \circ \varphi^{-1}$. But we have seen, that (e) is equivalent to (a) again.

The last equivalence to be proved is that of (b) and (d): Suppose (a), as φ is a split-epimorphism, there is some $\psi \in \mathcal{C}(Y,X)$, such that $\varphi \circ \psi = \mathbb{1}_Y$. Now compute $\varphi \circ (\psi \circ \varphi) = (\varphi \circ \psi) \circ \varphi = \mathbb{1}_Y \circ \varphi = \varphi = \varphi \circ \mathbb{1}_X$. As φ also is a monomorphism, we can conclude $\psi \circ \varphi = \mathbb{1}_X$ and thereby have (d). And from (d) we immediately get (f): An inverse map of $\varphi_* : \tau \mapsto \varphi \circ \tau$ is obviously given by $(\varphi^{-1})_* : \vartheta \mapsto \varphi^{-1} \circ \vartheta$. But we have seen, that (f) is equivalent to (a) again.

□

Proof of (11.11):
We first need to show, that $\Psi \circ \Phi$ is an isomorphism again with inverse $\Phi^{-1} \circ \Psi^{-1}$. Yet this can be done by a straightforward computation

$$\begin{aligned}
\big(\Psi \circ \Phi\big) \circ \big(\Phi^{-1} \circ \Psi^{-1}\big) &= \Psi \circ \big(\Phi \circ \Big(\Phi^{-1} \circ \Psi^{-1}\Big)\big) \\
&= \Psi \circ \big(\Big(\Phi \circ \Phi^{-1}\Big) \circ \Psi^{-1}\big) \\
&= \Psi \circ \big(\mathbb{1}_Y \circ \Psi^{-1}\big) \\
&= \Psi \circ \Psi^{-1} \;=\; \mathbb{1}_Z \\
\big(\Phi^{-1} \circ \Psi^{-1}\big) \circ \big(\Psi \circ \Phi\big) &= \big(\Big(\Phi^{-1} \circ \Psi^{-1}\Big) \circ \Psi\big) \circ \Phi \\
&= \big(\Phi^{-1} \circ \Big(\Psi^{-1} \circ \Psi\Big)\big) \circ \Phi \\
&= \big(\Phi^{-1} \circ \mathbb{1}_Y\big)\Phi \\
&= \Phi^{-1} \circ \Phi \;=\; \mathbb{1}_x
\end{aligned}$$

This second claim are the properties of an equivalence realtion of $\cong$. (1) Is easy, as $\mathbb{1}_X : X \cong X$ clearly is an isomorphism, due to $\mathbb{1}_X \circ \mathbb{1}_X = \mathbb{1}_X$. (2) If $\Phi : X \cong Y$ is an isomorphism, then Φ is the inverse of Φ^{-1}, as well. Hence $\Phi^{-1} : Y \cong X$ is the isomorphy that was claimed to persist. (3) If $\Phi : X \cong Y$ and $\Psi : Y \cong Z$ are isomorphisms, then we have shown above, that $\Psi \circ \Phi : X \cong Z$ is an isomorphy, as well. Hence all three properties are satisfied. □

Proof of (11.13):
As U is universal there is a unique morphism $\Phi : U \to V$, likewise as V is universal there is a unique morphism $\Psi : V \to U$. Hence $\Phi\Psi : U \to U$ is a morphism and as $\mathbb{1}_U : U \to U$ is another morphism the uniquess (U is universal) implies $\Phi\Psi = \mathbb{1}_U$. Likewise we find $\Psi\Phi = \mathbb{1}_V$ and hence $\Phi : U \to V$ is an isomorphism, with inverse morphism $\Psi : V \to U$. For terminal objects we can argue in complete analogy or simply note that terminal objects S and T of $\mathcal{C}$ are universal objects in $\mathcal{C}^{\mathrm{op}}$ such that $S \cong T$ in $\mathcal{C}^{\mathrm{op}}$ and therefore $S \cong T$ in $\mathcal{C}$. □

Proof of (11.14):

(i) Let T be any object of $\mathcal{C}$ and τ and $\tau' \in \mathcal{C}(T,X)$, such that $\varphi \circ \tau = \varphi \circ \tau'$. That is for any $t \in T$ we have $\varphi(\tau(t)) = \varphi(\tau'(t))$. As φ is injective, we get $\tau(t) = \tau'(t)$ from this and as this is true for any $t \in T$ this is $\tau = \tau'$ again. That is an injective morphism is an monomorphism.

Likewise for morphisms τ, $\tau' \in \mathcal{C}(Y,T)$ satisfying $\tau \circ \varphi = \tau' \circ \varphi$ we prove that the surjectivity of φ implies $\tau = \tau'$: Consider any $y \in Y$, as φ is surjective, there is some $x \in X$ such that $\varphi(x) = y$. And from this we get $\tau(y) = \tau \circ \varphi(x) = \tau' \circ \varphi(x) = \tau'(y)$. Again, as this is true for any $y \in Y$, we see $\tau = \tau'$ which is the property of an epimorphism.

(ii) Suppose $\varphi \in \mathcal{C}(X,Y)$ is a split-monomorphism. We have to verify that for any object T and any morphisms τ, $\tau' \in \mathcal{C}(T,X)$ with $\varphi \circ \tau = \varphi \circ \tau'$ we get $\tau = \tau'$. But by assumption there is some $\overline{\varphi} \in \mathcal{C}(Y,X)$ such that $\overline{\varphi} \circ \varphi = \mathbb{1}_X$. It suffices to apply such an $\overline{\varphi}$ to the equation, as this implies

$$\tau \;=\; \mathbb{1}_X \circ \tau \;=\; \big(\overline{\varphi} \circ \varphi\big) \circ \tau \;=\; \overline{\varphi} \circ \big(\varphi \circ \tau\big) \;=\; \overline{\varphi} \circ \big(\varphi \circ \tau'\big) \;=\; \big(\overline{\varphi} \circ \varphi\big) \circ \tau' \;=\; \mathbb{1}_X \circ \tau' \;=\; \tau'$$

Likewise for a split-epimorphism $\varphi \in \mathcal{C}(X,Y)$: We have to verify that for any object Z and any morphisms ζ, $\zeta' \in \mathcal{C}(Y,Z)$ with $\tau \circ \varphi = \zeta' \circ \varphi$ we get $\zeta = \zeta'$. But by assumption there is some $\overline{\varphi} \in \mathcal{C}(Y,X)$ such that $\varphi \circ \overline{\varphi} = \mathbb{1}_Y$. It suffices to apply such an $\overline{\varphi}$ to the equation, as this implies

$$\zeta \;=\; \zeta \circ \mathbb{1}_Y \;=\; \zeta \circ \big(\varphi \circ \overline{\varphi}\big) \;=\; \big(\zeta \circ \varphi\big) \circ \overline{\varphi} \;=\; \big(\zeta' \circ \varphi\big) \circ \overline{\varphi} \;=\; \zeta' \circ \big(\varphi \circ \overline{\varphi}\big) \;=\; \zeta' \circ \mathbb{1}_Y \;=\; \zeta'$$

(iii) If φ is a monomorphism, then for any object $T \in \mathrm{obj}(\mathcal{C})$ the map $\mathcal{C}(T,X) \hookrightarrow \mathcal{C}(T,Y) : \tau \mapsto \varphi \circ \tau$ is injective. And if φ is a monomorphism, as well, then the map $\mathcal{C}(X,Y) \hookrightarrow \mathcal{C}(X,Z) : \xi \mapsto \psi \circ \xi$ is injective, too. Hence the composition of these maps $\mathcal{C}(T,X) \hookrightarrow \mathcal{C}(T,Z) : \tau \mapsto \psi \circ (\varphi \circ \tau)$ is injective again. And as $\psi \circ (\varphi \circ \tau) = (\psi \circ \varphi) \circ \tau$ this injectivity is just what it takes to make $\psi \circ \varphi$ a monomorpism again. Conversely, if $\psi \circ \varphi$ is a monomorphism, let us prove, that φ has to be a monomorphism: That is we consider any τ, $\tau' \in \mathcal{C}(T,X)$ such that $\varphi \circ \tau = \varphi \circ \tau'$ and have to show $\tau = \tau'$. But this is easy: apply ψ from the left. As $\psi \circ \varphi$ is a monomorphism, we get $\tau = \tau'$ from

$$\big(\psi \circ \varphi\big) \circ \tau \;=\; \psi \circ \big(\varphi \circ \tau\big) \;=\; \psi \circ \big(\varphi \circ \tau'\big) \;=\; \big(\psi \circ \varphi\big) \circ \tau'$$

(iv) If ψ is an epimorphism, then for any object $T \in \mathrm{obj}(\mathcal{C})$ the map $\mathcal{C}(Z,T) \hookrightarrow \mathcal{C}(Y,T) : \tau \mapsto \tau \circ \psi$ is injective. And if φ is an epimorphism, as well, then the map $\mathcal{C}(Y,T) \hookrightarrow \mathcal{C}(X,Z) : \zeta \mapsto \zeta \circ \varphi$ is injective, too. Hence the composition of these maps $\mathcal{C}(Z,T) \hookrightarrow \mathcal{C}(X,T) : \tau \mapsto (\tau \circ \psi) \circ \varphi$ is injective again. And as $(\tau \circ \psi) \circ \varphi = \tau \circ (\psi \circ \varphi)$ this injectivity is just what it takes to make $\psi \circ \varphi$ an epimorpism again. Conversely, if $\psi \circ \varphi$ is an epimorphism, let us prove, that ψ has to be an epimorphism: That is we consider any τ, $\tau' \in \mathcal{C}(Z,T)$ such that $\tau \circ \psi = \tau' \circ \psi$ and have to show $\tau = \tau'$. But this is easy: apply φ from the right. As $\psi \circ \varphi$ is an epimorphism, we get $\tau = \tau'$ from

$$\tau \circ \big(\psi \circ \varphi\big) \;=\; \big(\tau \circ \psi\big) \circ \varphi \;=\; \big(\tau' \circ \psi\big) \circ \varphi \;=\; \tau' \circ \big(\psi \circ \varphi\big)$$

(v) As Y is an initial object, there is a uniquely defined morphism $\iota \in \mathcal{C}(Y,X)$. Thus $\mathbb{1}_Y$ and $\varphi \circ \iota$ both are morphisms in $\mathcal{C}(Y,Y)$. But as Y is an initial object, there is only one such morphism, such that $\varphi \circ \iota = \mathbb{1}_Y$. But from this we also get $\varphi \circ (\iota \circ \varphi) = (\varphi \circ \iota) \circ \varphi = \mathbb{1}_Y \circ \varphi = \varphi \circ \mathbb{1}_X$. And as φ is a monomorphism, this implies $\iota \circ \varphi = \mathbb{1}_X$. Together ι is the inverse morphism of φ.

(vi) As Y is a terminal object, there is a uniquely defined morphism $\pi \in \mathcal{C}(Z,Y)$. Thus $\mathbb{1}_Y$ and $\pi \circ \psi$ both are morphisms in $\mathcal{C}(Y,Y)$. But as Y is a terminal object, there is only one such morphism, such that $\pi \circ \psi = \mathbb{1}_Y$. But from this we also get $\mathbb{1}_Z \circ \psi = \psi \circ \mathbb{1}_Y = \psi \circ (\pi \circ \psi) = (\psi \circ \pi) \circ \psi$. And as ψ is an epimorphism, this implies $\mathbb{1}_Z = \psi \circ \pi$. Together π is the inverse morphism of ψ.

□

Proof of (11.15):

(i) If f is injective, then f has a left-inverse, by (0.10.(a)) and this already is the property of a split-monomorphism. A split-monomorphism already is a monomorphism, by (11.14.(ii)). So it remains to prove that a monomorphism f in **Set** is injective: Consider any two x, $x' \in X$, where $f : X \to Y$ and suppose $f(x) = f(x')$. Let T be a one-point set, e.g. $T = \{0\}$ and define $\tau : T \to X$ by $\tau(0) := x$ and $\tau' : T \to X$ by $\tau'(0) := x'$. Then we have $f\tau(0) = f(x) = f(x') = f\tau(0)$ such that $f\tau = f\tau'$. As f is assumed to be a monomorphism, we get $\tau = \tau'$, which is $x = \tau(0) = \tau'(0) = x'$. And this is the injectivity of f again.

- If f is surjective, then f has a right-inverse, by (0.10.(a)) and this already is the property of a split-epimorphism. A split-epimorphism already is an epimorphism, by (11.14.(ii)). So it remains to prove that an epimorphism f in **Set** is surjective: Suppose there was some $z \in Y$ with $z \in Y \setminus f(X)$, where $f : X \to Y$. Let $T := Y \sqcup \{t, t'\}$ where t and t' are any two distinct elements not contained in Y before, e.g. $t = (Y, 1)$ and $t' = (Y, 2)$. Now define $\tau : Y \to T$ by $\tau(y) := y$ for $y \neq z$ and $\tau(z) := t$ Likewise we let $\tau'(y) := y$ for $y \neq z$ and $\tau'(z) := t'$. As $z \in Y \setminus f(X)$, for any $x \in X$ we get $\tau f(x) = f(x) = \tau' f(x)$ such that $\tau f = \tau' f$. As f is assumed to be an epimorphism, we get $\tau = \tau'$, such that $t = \tau(z) = \tau'(z) = t'$. But this contradicts the construction of t and t', such that there cannot be any $z \in Y \setminus f(X)$. But this means $f(X) = Y$, which is the surjectivity of f.

(ii) If $\varphi : M \to N$ is injective, then φ already is a monomorphism, according to (11.14.(i)). Conversely, consider a monomorphism φ and any two x, $x' \in M$ such that $\varphi(x) = \varphi(x')$. We pick up $T := R$ as an R-module and define the homomorphisms $\tau : R \to M$ by $\tau(a) := ax$ and $\tau' : R \to M$ by $\tau'(a) := ax'$. As φ is R-linear, we get $\varphi\tau(a) = \varphi(ax) = a\varphi(x) = a\varphi(x') = \varphi(ax') = \varphi\tau'(a)$. That is $\varphi\tau = \varphi\tau'$ and hence $\tau = \tau'$, as φ was assumed to be a monomorphism. In particular $x = \tau(1) = \tau'(1) = x'$, which is the injectivity of φ.

- If $\varphi : M \to N$ is surjective, then φ already is an epimorphism, according to (11.14.(i)). Conversely, consider an epimorphism φ and define the R-module $T := N/\mathrm{im}(\varphi)$. Now regard the homomorphisms $\tau : N \to T : y \mapsto 0$ and $\tau' : N \to T : y \mapsto y + \mathrm{im}(\varphi)$. For any $x \in M$ we get $\tau\varphi(x) = 0 = 0 + \mathrm{im}(\varphi) = \varphi(x) + \mathrm{im}(\varphi) = \tau'\varphi(x)$, such that $\tau\varphi = \tau'\varphi$. As φ is an epimorphism, this implies $\tau = \tau'$ and this is $0 = \tau(y) = \tau'(y) = y + \mathrm{im}(\varphi)$ for any $y \in N$. In other words $y \in \mathrm{im}(\varphi)$ and thereby φ is surjective, as $y \in N$ is arbitrary.

- If $\varphi : M \to N$ is a bijective homomorphism, then φ is an isomorphism with inverse $\varphi^{-1} : N \to M$, according to (3.77.(b)). Conversely, if φ is an isomorphism, then there is a inverse morphism $\psi : N \to M$ of φ. In particular Ψ is the inverse map of φ and thereby φ is bijective.

(iii) If $\varphi : R \to S$ is injective, then φ already is a monomorphism, according to (11.14.(i)). Conversely, consider a monomorphism $\varphi : R \to S$, we have to verify, that φ is injective: Hence we consider any two elements a, $a' \in R$ such that $\varphi(a) = \varphi(a')$. Take the polynomial ring $T := \mathbb{Z}[t]$ and define the homomorphisms $\tau : T \to R : f \mapsto f(a)$ and likewise $\tau' : T \to R : f \mapsto f(a')$. As φ is a homomorphism of rings we get $\varphi\tau(f) = \varphi(f(a)) = f(\varphi(a)) = f(\varphi(a')) = \varphi(f(a')) = \varphi\tau'(f)$ for any $f \in T$, such that $\varphi\tau = \varphi\tau'$. As φ is a monomorphism we conclude $\tau = \tau'$ and thereby $a = \tau(t) = \tau'(t) = a'$, which is the injectivity of φ.

- If $\varphi : R \to S$ is a bijective homomorphism, then φ is an isomorphism with inverse $\varphi^{-1} : S \to R$, according to (1.80.(ii).(b)). Conversely, if φ is an isomorphism, then there is an inverse morphism

$\psi : S \to R$ of φ. In particular ψ is the inverse map of φ and thereby φ is bijective.

- Let us verify, that $\zeta(k) := k/1$ is an epimorphism $\mathbb{Z} \to \mathbb{Q}$. Consider any ring T and τ, $\tau' : \mathbb{Q} \to T$ such that $\tau\zeta = \tau'\zeta$. First of all, note that $1_T = \tau(1/1) = \tau(b/b) = \tau(b/1)\tau(1/b)$. That is for any $b \neq 0$ we have $\tau\zeta(b) = \tau(b/1) \in T^*$. Also note that for any $a \in \mathbb{Z}$ we have $\tau(a/1) = \tau\zeta(a) = \tau'\zeta(a) = \tau'(a/1)$. But for any $b \neq 0$ we thereby also get

$$\tau\left(\frac{b}{1}\right)\tau\left(\frac{a}{b}\right) \;=\; \tau\left(\frac{b}{1}\frac{a}{b}\right) \;=\; \tau\left(\frac{a}{1}\right) \;=\; \tau'\left(\frac{a}{1}\right) \;=\; \tau'\left(\frac{b}{1}\frac{a}{b}\right) \;=\; \tau'\left(\frac{b}{1}\right)\tau'\left(\frac{a}{b}\right)$$

 As $\tau(b/1) = \tau'(b/1)$ is a unit in T we conclude $\tau(a/b) = \tau'(a/b)$ for any $a \in \mathbb{Z}$ and $b \neq 0$. That is for any $a/b \in \mathbb{Q}$ and hence $\tau = \tau'$. In particular ζ is an epimorphism in **Ring**.

(iv) As all these categories are concrete, injective morphisms are monomorphisms and surjective morphisms are epimorphisms, according to (11.14.(i)). And isomorphisms trivially are bijective morphisms, as the inverse morphism also is an inverse map. Thus for all these categories, in any equivalence we only have to check one direction.

 For **Set** we have already seen in (i), that any monomorphism is injective and any epimorphism is surjective. And for a bijective morphism the inverse map also is an inverse morphism, as any map is a morphism in this category.

- Let us regard **Group** next and start with a monomorphism $\varphi : G \to H$. We have to verify, that φ is injective: Hence we consider any two elements x, $x' \in G$ such that $\varphi(x) = \varphi(x')$. Take $T := \mathbb{Z}$ and define the homomorphisms $\tau : \mathbb{Z} \to G : k \mapsto x^k$ and likewise $\tau' : \mathbb{Z} \to G : k \mapsto x'^k$. Then it is clear, that for any $k \in \mathbb{Z}$ we get $\varphi\tau(k) = \varphi(x^k) = \varphi(x)^k = \varphi(x')^k = \varphi(x'^k) = \varphi\tau'(k)$ such that $\varphi\tau = \varphi\tau'$. As φ is a monomorphism we conclude $\tau = \tau'$ and thereby $x = \tau(1) = \tau'(1) = x'$, which is the injectivity of φ.

 Now for an epimorphism $\varphi : G \to H$: Let us abbreviate $P := \mathrm{im}(\varphi)$ which is a subgroup of H. Then we can regard $X := H/P$ as a set. Pick up another element ∞ not in X before, e.g. $\infty := X$, and let $Y := X \cup \{\infty\}$. Then we consider the permutation group

$$T \;:=\; S_Y$$

 Let $\sigma \in T$ be the transposition $\sigma := (eP\ \infty)$. We can turn any element $h \in H$ into a permutation on X by multiplication from the left. Clearly this is an (even injective) homomorphism of groups. And thereby we find a homomorphism of groups of the form

$$\tau \;:\; H \to T \;:\; k \mapsto \begin{cases} y \mapsto khP \text{ if } y = hP \in X \\ \qquad\quad \infty \text{ if } y = \infty \notin X \end{cases}$$

 We define another homomorphism of groups τ' by conjugating τ with the transposition $\sigma \in T$, i.e.

$$\tau \;:\; H \to T \;:\; k \mapsto \sigma\tau(k)\sigma^{-1}$$

 Consider any $g \in G$ and compute $\tau(\varphi(g))(eP)$. By construction this is $\varphi(g)eP = \varphi(g)P = eP$, as $\varphi(g) \in P$. That is eP is fixed under $\tau(\varphi(g))$. But so is ∞ and hence $\tau(\varphi(g))$ and σ have disjoint

domains. Therefore they commute, according to (1.14.(iii)). That is we have $\sigma\tau(\varphi(g)) = \tau(\varphi(g))\sigma$ and thereby $\tau'(\varphi(g)) = \sigma\tau(\varphi(g))\sigma^{-1} = \tau(\varphi(g))$ for any $g \in G$. In other words that is $\tau'\varphi = \tau\varphi$ and as φ was assumed to be an epimorphism, this implies $\tau' = \tau$. That is for any $k \in H$ we have

$$\sigma\tau(k)\sigma^{-1} \;=\; \tau'(k) \;=\; \tau(k)$$

and thereby $\sigma\tau(k) = \tau(k)\sigma$ commute. Suppose there was some $k \in H$ with $tP := \tau(k)(eP) \neq eP$. As σ only acts on eP and ∞ but tP is neither, we then had $\sigma\tau(k)(eP) = \sigma(tP) = tP$. But on the other hand we then also had $\tau(k)\sigma(eP) = \tau(k)(\infty) = \infty$. But now $tP \neq \infty$ contradicts $\sigma\tau(k)(eP) = \tau(k)\sigma(eP)$ and hence this cannot be. We conclude that is eP has to be fixed under any $\tau(k)$, for any $k \in H$. In other words $eP = \tau(k)(eP) = keP = kP$, which is $k \in P = \mathrm{im}(\varphi)$. As this is true for any $k \in H$, we find that φ truly has to be surjective.

If $\varphi : G \to H$ is a bijective homomorphism of groups, then its inverse is a homomorphism of groups again. This can be done in the standard way: Consider any $x, y \in H$, as φ is surjective, there are $u, v \in G$ such that $x = \varphi(u)$ and $y = \varphi(v)$. Using these we are able to compute

$$\varphi^{-1}(xy) \;=\; \varphi^{-1}\big(\varphi(u)\varphi(v)\big) \;=\; \varphi^{-1}\big(\varphi(uv)\big) \;=\; uv \;=\; \varphi^{-1}(x)\varphi^{-1}(y)$$

As $\varphi\varphi^{-1} = \mathbb{1}_H$ and $\varphi^{-1}\varphi = \mathbb{1}_G$ is clear for the inverse function and φ^{-1} inherits the properties of a homomorphism of groups from φ we see, that φ^{-1} is the inverse morphism of φ.

- The case $\mathbf{Alg}_R$ is much the same, as for **Ring**: If A and B are R-algebras and $\varphi : A \to B$ is a momonorphism, then take to the polynomial ring $T := R[t]$, which is an R-algebra again, as R is commutative. We have to verify, that φ is injective: Hence we consider any two elements $u, u' \in A$ such that $\varphi(u) = \varphi(u')$ and define the homomorphisms $\tau : T \to A : f \mapsto f(u)$ and likewise $\tau' : T \to A : f \mapsto f(u')$. As φ is a homomorphism of R-algebras can compute again: $\varphi\tau(f) = \varphi(f(u)) = f(\varphi(u)) = f(\varphi(u')) = \varphi(f(u')) = \varphi\tau'(f)$ for any $f \in T$, such that $\varphi\tau = \varphi\tau'$. As φ is a monomorphism we conclude $\tau = \tau'$ and thereby $u = \tau(t) = \tau'(t) = u'$, which is the injectivity of φ.

 If $\varphi : A \to B$ is a bijective homomorphism, then the inverse map φ^{-1} is both, a homomorphism of rings and of R-modules, according to (1.80.(ii).(b)) and (3.77.(b)) respectively. Together φ^{-1} is a homomorphism of R-algebras and thereby φ is an isomorphism. Conversely, if φ is an isomorphism, then there is an inverse morphism $\psi : B \to A$ of φ. In particular ψ is the inverse map of φ and thereby φ is bijective.

□

Proof of (11.17):

- Let us first prove that $\varphi \mid \psi$ is reflexive and transitive: For any $\psi \in \mathcal{C}(X, Z)$ we clearly have $\psi = \psi \circ \mathbb{1}_X$ and thereby $\psi \mid \psi$. And if $\psi_1 \mid \psi_2$ and $\psi_2 \mid \psi_3$ then by definition there are $\psi_1' \in \mathcal{C}(X_1, X_2)$ and $\psi_2' \in \mathcal{C}(X_2, X_3)$ such that $\psi_3 = \psi_2 \circ \psi_2'$ and $\psi_2 = \psi_1 \circ \psi_1'$. Combining these we find $\psi_3 = (\psi_1 \circ \psi_1') \circ \psi_2' = \psi_1 \circ (\psi_1' \circ \psi_2')$ and thereby $\psi_1 \mid \psi_3$.

 The properties of an equivalence relation are straightforward: We get (1) from the reflexivity of the factors relation. Property (2) is trivial, as the relation $\sim$ has been defined by a symmetric condition. And (3) is clear by the transitivity of the factors relation - just pair the factors relations.

- *Uniquely determined*: Now suppose $\psi_2 = \psi_1 \circ \psi_1'$ where ψ_1 and ψ_2 are monomorphisms. Also suppose there was another $\psi_1'' \in \mathcal{C}(X_2, X_1)$ such that $\psi_2 = \psi_1 \circ \psi_1''$. Then we had $\psi_1 \circ \psi_1' = \psi_1 \circ \psi_1''$ and as ψ_1 is a monomorphism, we conclude $\psi_1' = \psi_1''$. That is ψ_1' is uniquely determined and in complete analogy we see, that ψ_2' is uniquely determined, as ψ_2 is a monomorphism, too.

- *Mutually inverse*: By assumption we have $\psi_2 = \psi_1 \circ \psi_1'$ and $\psi_1 = \psi_2 \circ \psi_2'$. Plugging the first equation into the second, we see $\psi_1 \circ \mathbb{1}_{X_1} = \psi_1 = (\psi_1 \circ \psi_1') \circ \psi_2' = \psi_1 \circ (\psi_1' \circ \psi_2')$. As ψ_1 is a monomorphism, this yields $\mathbb{1}_{X_1} = \psi_1' \circ \psi_2'$ and the other way around we also find $\mathbb{1}_{X_2} = \psi_2' \circ \psi_1'$. That is the morphisms ψ_1' and ψ_2' are the inverse morphism of one and another.

□

Proof of (11.20):
The first equality is easy: $\psi \circ 0 = \psi \circ (0+0) = \psi \circ 0 + \psi \circ 0$. Subtracting one $\psi \circ 0$ from this equation we end up at $0 = \psi \circ 0$. In complete analogy we can prove $0 = 0 \circ \varphi$.
Using the first two equations we can also prove the second two equations: $0 = \psi \circ 0 = \psi \circ (\varphi + (-\varphi)) = \psi \circ \varphi + \psi \circ (-\varphi)$. Subtracting $\psi \circ \varphi$ from this equation we end up with $-(\psi \circ \varphi) = \psi \circ (-\varphi)$ and in complete analogy we can prove $-(\psi \circ \varphi) = (-\psi) \circ \varphi$. □

Proof of (11.26):

(i) Let $\Phi^{-1} \in \mathcal{C}(Y, X)$ be the inverse morphism of Φ, then we have $\Phi^{-1} \circ \Phi = \mathbb{1}_X$ and $\Phi \circ \Phi^{-1} = \mathbb{1}_Y$. In particular $\mathbb{1}_{F(X)} = F(\mathbb{1}_X) = F(\Phi^{-1} \circ \Phi) = F(\Phi^{-1}) \circ F(\Phi)$. In complete analogy we find that $\mathbb{1}_{F(Y)} = F(\Phi) \circ F(\Phi^{-1})$. Thus we see that $F(\Phi^{-1})$ is the inverse morphism of $F(\Phi)$ and in particular $F(\Phi)$ is invertible.

(ii) As F is full, there are some morphisms Φ and Ψ of $\mathcal{C}$ such that $F(\Phi) = \Theta$ and $F(\Psi) = \Theta^{-1}$. For these morphisms we find $F(\Phi \circ \Psi) = F(\Phi) \circ F(\Psi) = \Theta \circ \Theta^{-1} = \mathbb{1}_{F(Y)} = F(\mathbb{1}_Y)$. As F also is faithful, we get $\Phi \circ \Psi = \mathbb{1}_Y$ from this. In complete analogy we find $\Psi \circ \Phi = \mathbb{1}_X$ and thereby Φ is an isomorphism of $\mathcal{C}$ with inverse morphism Φ. This isomorphism is uniquely determined by $F(\Phi) = \Theta$, as F is faithful.

(iii) Let us abbreviate $D := F(X) = F(Y)$. Clearly $\mathbb{1}_D$ is an isomorphism $\mathbb{1}_D : D \xrightarrow{\sim} D$. Now by (ii) there is an isomorphism $\Phi : X \xrightarrow{\sim} Y$ such that $F(\Phi) = \mathbb{1}_D$. In particular $X \cong Y$ are isomorphic.

□

Proof of (11.31):

(i) Property (1) is obvious: If $E = \mathbb{1}$ and $\overline{E} = \mathbb{1}$ is the identity functor on $\mathcal{C}$, then the isomorphisms $\Phi_X : X \xrightarrow{\sim} \overline{E}E(X) = X$ are just the identities $\Phi_X = \mathbb{1}_X$ and likewise for Θ_X. Property (2) is trivial, as the properties (1), (2) and (3), (4) of an equivalence of categories are symmetric under interchanging E and $\overline{E}$. The only property that requires a little effort is the transitivity (3): Consider any two objects U, $U' \in \mathrm{obj}(\mathcal{B})$ and a morphism $\varphi \in \mathcal{B}(U, U')$. By assumption $(D, \overline{D}) : \mathcal{B} \sim \mathcal{C}$ there are isomorphisms $\Gamma_U : U \xrightarrow{\sim} \overline{D}D(U)$ such that the following diagram commutes

$$\begin{array}{ccc} U & \xrightarrow{\Gamma_U} & \overline{D}(D(U)) \\ \downarrow & & \downarrow \\ U' & \xrightarrow{\Gamma_{U'}} & \overline{D}(D(U')) \end{array}$$

Let $X := D(U)$, $X' := D(U')$ and $\psi := D(\varphi) \in \mathcal{C}(X, X')$. Then by assumption $(E, \overline{E}) : \mathcal{C} \sim \mathcal{D}$ there are isomorphisms $\Phi_X : X \xrightarrow{\sim} \overline{E}E(X)$ such that the following diagram commutes, as well

$$\begin{array}{ccc} X & \xrightarrow{\Phi_X} & \overline{E}(E(X)) = \overline{E}ED(U) \\ \downarrow & & \downarrow \\ X' & \xrightarrow{\Phi_{X'}} & \overline{E}(E(X')) = \overline{E}ED(U') \end{array}$$

Apply the functor $\overline{D}$ to this diagram, by (11.26) the isomorphisms Φ_X (from left to right) remain isomorphisms and the commutativity is preserved by functors, as well. Then we may compose these diagrams to find

$$\begin{array}{ccccc} U & \xrightarrow{\Gamma_U} & \overline{D}(D(U)) = \overline{D}(X) & \xrightarrow{\overline{D}(\Phi_X)} & \overline{D}\overline{E}ED(U) \\ \downarrow & & \downarrow & & \downarrow \\ U' & \xrightarrow{\Gamma_{U'}} & \overline{D}(D(U')) = \overline{D}(X') & \xrightarrow{\overline{D}(\Phi_{X'})} & \overline{D}\overline{E}ED(U') \end{array}$$

Hereby the morphisms pointing top-down are φ, $\overline{D}(\psi) = D(\varphi)$ and $\overline{D}\overline{E}ED(\varphi)$. Hence we find a family of isomorphisms $\overline{D}(\Phi_{D(U)})\Gamma_U : U \xrightarrow{\sim} \overline{D}\overline{E}ED(U)$ that yield commutative diagrams with morphimsm $\varphi : U \to U'$. That is ED satisfies property (3) of an equivalence of categories. By the symmetry of property (4), it is clear that we also find compatible isomorphisms $Y \xrightarrow{\sim} ED\overline{D}\overline{E}$ such that property (4) is satisfied, as well. Altogether $(ED, \overline{D}\overline{E}) : \mathcal{B} \sim \mathcal{D}$ is an equivalence of categories.

(ii) We start by proving that E is faithful, that is we regard any two objects X, $X' \in \mathrm{obj}(\mathcal{C})$ and let $Y := E(X)$ and $Y' := E(X')$. Then we have to prove, that the following map is injective

$$\mathcal{C}(X, X') \to \mathcal{D}(Y, Y') \; : \; \varphi \mapsto E(\varphi)$$

But by assumption we have another functor $\overline{E} : \mathcal{D}(Y, Y') \to \mathcal{C}(Z, Z')$ where we let $Z := \overline{E}(Y)$ and $Z' := \overline{E}(Y')$ satisfying $\overline{E}E(\varphi) = \Phi_{X'}\,\varphi\,\Phi_X^{-1}$ for some isomorphisms $\Phi_{X'}$ and Φ_X. So supposed we had some morphisms φ_1, $\varphi_2 \in \mathcal{C}(X, X')$ such that $E(\varphi_1) = E(\varphi_2)$, then we could apply $\overline{E}$ to find

$$\Phi_{X'}\,\varphi_1\,\Phi_X^{-1} \; = \; \overline{E}E(\varphi_1) \; = \; \overline{E}E(\varphi_2) \; = \; \Phi_{X'}\,\varphi_2\,\Phi_X^{-1}$$

But as $\Phi_{X'}$ and Φ_X are isomorphisms we hence get $\varphi_1 = \varphi_2$ which is the injectivity of E on the morphisms. That is E is faithful. In complete analogy we find, that $\overline{E}$ is faithful, too. To prove that E also is full we regard any morphism $\psi \in \mathcal{D}(Y, Y')$ where $Y := E(X)$ and $Y' := E(X')$ and X, $X' \in \mathrm{obj}(\mathcal{C})$ are arbitrary. Then we have to find some morphism $\varphi \in \mathcal{C}(X, X')$, such that $E(\varphi) = \psi$. But if we define

$$\varphi \; := \; \Phi_{X'}^{-1}\,\overline{E}(\psi)\,\Phi_X$$

then we have $\overline{E}E(\varphi) = \Phi_{X'}\,\varphi\,\Phi_X^{-1} = \overline{E}(\psi)$. But as $\overline{E}$ is faithful, we conclude, that $E(\varphi) = \psi$. And this is just what we needed for E being full. In complete analogy, we see, that $\overline{E}$ is full, as well. It remains to prove that E (and likewise $\overline{E}$) are essentially surjective: That is we are given any object $Y \in \mathrm{obj}(\mathcal{D})$ and need to find an object $X \in \mathrm{obj}(\mathcal{C})$, such that $E(X) \cong Y$. It stands to reason to take $X := \overline{E}(Y)$, then by property (4) of an equivalence of categories there is an isomorphism $\Theta_Y : Y \xrightarrow{\sim} E\overline{E}(Y) = E(X)$, which is just what we needed. Clearly the essential surjectivity of $\overline{E}$

follows from the analogous argument and property (3).

(iii) Let us first construct $\overline{E}$: Given any object $Y \in \mathrm{obj}(\mathcal{D})$ we can choose an object $X_Y \in \mathrm{obj}(\mathcal{C})$ and a morphism Θ_Y, such that $\Theta_Y : Y \xrightarrow{\sim} E(X_Y)$ is an isomorphism. This is due to the essential surjectivity of E. Thus we let $\overline{E}(Y) := X_Y$ and thereby get

$$\Theta_Y \ : \ Y \ \xrightarrow{\sim} \ E\overline{E}(Y)$$

Now consider a morphism $\psi \in \mathcal{D}(Y, Y')$ and abbreviate $X := \overline{E}(Y)$ and $X' := \overline{E}(Y')$. The following diagram commutes if the top-down maps are taken to be ψ and $\Theta_{Y'} \circ \psi \circ \Theta_Y^{-1}$ respectively:

$$\begin{array}{ccc} Y & \xrightarrow{\Theta_Y} & E(X) \\ \downarrow & & \downarrow \\ Y' & \xrightarrow{\Theta_{Y'}} & E(X') \end{array}$$

That is $\Theta_{Y'} \circ \psi \circ \Theta_Y^{-1} \in \mathcal{D}(E(X), E(X'))$. As E is full and faithful, there is a uniquely determined morphism $\varphi \in \mathcal{C}(X, X')$ such that $E(\varphi) = \Theta_{Y'} \circ \psi \circ \Theta_Y^{-1}$. We then define $\overline{E}(\psi) := \varphi$, that is $\overline{E}(\psi)$ is uniquely defined by the property

$$E\big(\overline{E}(\psi)\big) \ = \ \Theta_{Y'} \circ \psi \circ \Theta_Y^{-1}$$

We first have to check, that this definition of $\overline{E}$ truly yields a functor. That is we have to verify, that for any two morphisms $\psi_1 \in \mathcal{D}(Y_1, Y_2)$ and $\psi_2 \in \mathcal{D}(Y_2, Y_3)$ we get $\overline{E}(\psi_2 \circ \psi_1) = \overline{E}(\psi_2) \circ \overline{E}(\psi_1)$. However it is clear, that

$$\Theta_{Y_3} \circ \big(\psi_2 \circ \psi_1\big) \circ \Theta_{Y_1}^{-1} \ = \ \big(\Theta_{Y_3} \circ \psi_2 \circ \Theta_{Y_2}^{-1}\big) \circ \big(\Theta_{Y_2} \circ \psi_1 \circ \Theta_{Y_1}^{-1}\big)$$

That is $E\overline{E}(\psi_2 \circ \psi_1) = E\overline{E}(\psi_2) \circ E\overline{E}(\psi_1) = E(\overline{E}(\psi_2) \circ \overline{E}(\psi_1))$. And as E is faithful, we can strip E and find the functorial property $\overline{E}(\psi_2 \circ \psi_1) = \overline{E}(\psi_2) \circ \overline{E}(\psi_1)$. Property (4) of equivalences of categories is already satisfied by the definition of $\overline{E}(\psi)$. It only remains to verify property (3), that is we have to construct the isomorphisms $\Phi_X : X \xrightarrow{\sim} \overline{E}E(X)$: Given any object $X \in \mathrm{obj}(\mathcal{C})$ let $X' := X_{E(X)} = \overline{E}E(X)$. Then

$$\Theta_{E(X)} \ : \ E(X) \ \xrightarrow{\sim} \ E\overline{E}\big(E(X)\big) = E(X')$$

is an isomorphism. As E is full and faithful this implies, that there is a uniquely determined isomorphism $\Phi_X : X \xrightarrow{\sim} X' = \overline{E}E(X)$ satisfying $E(\Phi_X) = \Theta_{E(X)}$, according to (11.26.(ii)). Now consider any morphism $\varphi \in \mathcal{C}(X, X')$, we have to verify the commutativity of the diagram in property (3). Just apply the functor E and abbreviate $\psi := E(\varphi)$, then we will verify the commutativity of the following diagram

$$\begin{array}{ccc} E(X) & \xrightarrow{\psi} & E(X') \\ \downarrow & & \downarrow \\ E\overline{E}E(X) & \xrightarrow{E\overline{E}(\psi)} & E\overline{E}E(X') \end{array}$$

The top-down maps have been Φ_X and $\Phi_{X'}$ respectively. Under E they turned into $\Theta_{E(X)}$ and

$\Theta_{E(X')}$. And by construction $E\overline{E}(\psi)$ is $\Theta_{E(X')} \circ \psi \circ \Theta^{-1}_{E(X)}$. That is the above diagram *is* commutative. But as E is faithful we can strip E again and this means the diagram in property (3) is commutative. Altogether we have proved, that $(E, \overline{E})$ satisfies the properties of an equivalence of categories.

(iv) This statement is purely definitional: In (a) $\Longrightarrow$ (b) property (3) of the equivalence of categories yields a collection $\Phi = (\Phi_X)$ of morphisms, which is a natural transformation $\Phi : \mathbb{1}_{\mathcal{C}} \rightrightarrows \overline{E}E$. And as all the $\Phi_X : X \xrightarrow{\sim} \overline{E}E(X)$ are assumed to be isomorphisms, this Φ is a natural isomorphism. Likewise property (4) of the equivalence of categories makes $\Theta = (\Theta_Y)$ a natural isomorphism of the form $\Theta : \mathbb{1}_{\mathcal{D}} \rightrightarrows E\overline{E}$. Conversely, for (b) $\Longrightarrow$ (a), to say that $\Phi : \mathbb{1}_{\mathcal{C}} \rightrightarrows \overline{E}E$ is a natural transformation, is the commutativity in property (3) again. And as Φ is a natural isomorphism, any Φ_X is an isomorphism. And the same is true for the natural isomorphism $\Theta : \mathbb{1}_{\mathcal{D}} \rightrightarrows E\overline{E}$, of course.

□

Proof of (11.33):

(i) Clearly $\varphi = \mathbb{1}_P$ is a morphism $\mathbb{1}_P : P \to P$ satisfying $\pi_i = \pi_i \circ \varphi$. And as (P, π_i) is a product of the X_i this has to the *only* morphism $\varphi \in \mathcal{C}(P, P)$ that makes all these diagrams commute. Now apply (3) to (P', π'_i), then we find a morphism $\pi' : P' \to P$ such that $\pi'_i = \pi_i \circ \pi'$.

Likewise (P', π'_i) is a product of the X_i so by the same reasoning, as above, we see that $\varphi' = \mathbb{1}_{P'} \in \mathcal{C}(P', P')$ is the one and only morphism making all the diagrams $\pi'_i = \pi'_i \circ \varphi'$ commute. And applying (3) to (P, π_i) we also find a morphism $\pi : P \to P'$ such that $\pi_i = \pi'_i \circ \pi$.

Let us now compose these morphisms π' and π: We find $\pi_i \circ (\pi' \circ \pi) = (\pi_i \circ \pi') \circ \pi = \pi'_i \circ \pi = \pi_i$. That is $\varphi = \pi' \circ \pi$ always satisfies $\pi_i \circ \varphi = \pi_i$ and thereby we conclude $\pi' \circ \pi = \mathbb{1}_P$. In complete analogy we find $\pi'_i \circ (\pi \circ \pi') = (\pi'_i \circ \pi) \circ \pi' = \pi_i \circ \pi' = \pi'_i$ such that $\varphi' = \pi \circ \pi'$ always satisfies $\pi'_i \circ \varphi' = \pi'_i$. Again we get $\pi \circ \pi' = \mathbb{1}_{P'}$ and thereby π and π' are mutually inverse. In particular $\pi : P \xrightarrow{\sim} P'$ is an isomorphism. And by construction $\Phi := \pi$ is the uniquely determined morphism, satisfying $\pi_i = \pi'_i \circ \Phi$ for any $i \in I$.

(ii) The proof follows exactly the same lines, as the proof of (i) above. We present it for completeness purposes, only: Clearly $\varphi = \mathbb{1}_S$ is a morphism $\mathbb{1}_S : S \to S$ satisfying $\varepsilon_i = \varphi \circ \varepsilon_i$. And as (S, ε_i) is a coproduct of the X_i this has to the *only* morphism $\varphi \in \mathcal{C}(S, S)$ that makes all these diagrams commute. Now apply (3) to (S', ε'_i), then we find a morphism $\varepsilon' : S \to S'$ such that $\varepsilon'_i = \varepsilon' \circ \varepsilon_i$.

Likewise (S', ε'_i) is a coproduct of the X_i so by the same reasoning, as above, we see that $\varphi' = \mathbb{1}_{S'} \in \mathcal{C}(S', S')$ is the one and only morphism making all the diagrams $\varepsilon'_i = \varphi' \circ \varepsilon'_i$ commute. And applying (3) to (S, ε_i) we also find a morphism $\varepsilon : S' \to S$ such that $\varepsilon_i = \varepsilon \circ \varepsilon'_i$.

Let us now compose these morphisms ε' and ε: Again we find $(\varepsilon \circ \varepsilon') \circ \varepsilon_i = \varepsilon \circ (\varepsilon' \circ \varepsilon_i) = \varepsilon \circ \varepsilon'_i = \varepsilon_i$. That is $\varphi = \varepsilon \circ \varepsilon'$ always satisfies $\varphi \circ \varepsilon_i = \varepsilon_i$ and thereby we conclude $\varepsilon \circ \varepsilon' = \mathbb{1}_S$. In complete analogy we find $(\varepsilon' \circ \varepsilon) \circ \varepsilon'_i = \varepsilon' \circ (\varepsilon \circ \varepsilon'_i) = \varepsilon' \circ \varepsilon_i = \varepsilon'_i$ such that $\varphi' = \varepsilon' \circ \varepsilon$ always satisfies $\varphi' \circ \varepsilon'_i = \varepsilon'_i$. Again we get $\varepsilon' \circ \varepsilon = \mathbb{1}_{S'}$ and thereby ε and ε' are mutually inverse. In particular $\varepsilon : S \xrightarrow{\sim} S'$ is an isomorphism. And by construction $\Phi := \varepsilon$ is the uniquely determined morphism, satisfying $\varepsilon'_i = \Phi \circ \varepsilon_i$ for any $i \in I$.

(iii) Let us first prove (b) $\Longrightarrow$ (a) for products: To prove that (P, π_i) is a product of the X_i we consider some $U \in \mathrm{obj}(\mathcal{C})$ and some $\varphi_i \in \mathcal{C}(U, X_i)$ and have to find a uniquely determined $\varphi \in \mathcal{C}(U, P)$ such

that $\pi_i \circ \varphi = \varphi_i$ for any $i \in I$. So apply E to this diagram, that is $E(\pi_i) \in \mathcal{D}(E(P), E(X_i))$ and $E(\varphi_i) \in \mathcal{D}(E(U), E(X_i))$. As $(E(P), E(\pi_i))$ is a product of the $E(X_i)$ there is a uniquely determined morphism $\psi \in \mathcal{D}(E(U), E(P))$ such that $E(\pi_i) \circ \psi = E(\varphi_i)$ for any $i \in I$. By (11.31.(ii)) E is full and faithful, that is

$$\mathcal{C}(U,P) \;\longleftrightarrow\; \mathcal{D}\big(E(U),E(P)\big) \;:\; \varphi \mapsto E(\varphi)$$

is bijective. And thereby there is a uniquely determined $\varphi \in \mathcal{C}(U,P)$ such that $E(\varphi) = \psi$. Suppose there was another $\varphi' \in \mathcal{C}(U,P)$ such that $\pi_i \circ \varphi' = \varphi_i$ for any $i \in I$. Applying E to this diagram we get $E(\pi_i) \circ E(\varphi') = E(\varphi_i)$ and thereby $E(\varphi') = \psi = E(\varphi)$. Thus we find $\varphi' = \varphi$ and thereby we have found a uniquely determined φ, as needed for the product property.

(iii) Conversely, let us prove (a) $\Longrightarrow$ (b) for products: To prove that $(E(P), E(\pi_i))$ is a product of the $E(X_i)$ we consider any $V \in \mathrm{obj}(\mathcal{D})$ and some $\psi_i \in \mathcal{D}(V, E(X_i))$ and have to find a uniquely determined $\psi \in \mathcal{D}(V, E(P))$ such that $E(\pi_i) \circ \psi = \psi_i$ for any $i \in I$. By (11.31.(ii)) E not only is full and faithful, but also essentially surjective. That is, there is some $U \in \mathrm{obj}(\mathcal{C})$ such that $\Phi : E(U) \xrightarrow{\sim} V$ are isomorphic. Then $\psi_i \circ \Phi : E(U) \to E(X_i)$ is a morphism, such that by assumption (a) there is a uniquely determined morphism $\varphi_i : U \to X_i$ such that $E(\varphi_i) = \psi_i \circ \Phi$. As P is a product of the X_i there is a uniquely determined $\varphi : U \to P$ such that $\pi_i \circ \varphi = \varphi_i$ for any $i \in I$. Applying E to these diagrams, we get

$$E(\pi_i) \circ E(\varphi) \;=\; E\big(\pi_i \circ \varphi\big) \;=\; E(\varphi_i) \;=\; \psi_i \circ \Phi$$

Now define $\psi := E(\varphi) \circ \Phi^{-1}$ then by the equation above we have $E(\pi_i) \circ \psi = \psi_i$ for any $i \in I$. Thus the existence of ψ is established. Suppose there was another $\psi' \in \mathcal{D}(V, E(P))$ such that $E(\pi_i) \circ \psi' = \psi_i$ for any $i \in I$. Then $\psi' \circ \Phi \in \mathcal{D}(E(U), E(P))$ which corresponds to $\mathcal{C}(U,P)$. That is there is some $\varphi' \in \mathcal{C}(U,P)$ such that $E(\varphi') = \psi' \circ \Phi$. Then we get

$$E(\varphi_i) \;=\; \psi_i \circ \Phi \;=\; \big(E(\pi_i) \circ \psi'\big) \circ \Phi \;=\; E(\pi_i) \circ \big(\psi' \circ \Phi\big) \;=\; E(\pi_i) \circ E(\varphi') \;=\; E\big(\pi_i \circ \varphi'\big)$$

From this we find $\varphi_i = \pi_i \circ \varphi'$ and as this is true for any $i \in I$ and φ is unique with this property, we see $\varphi' = \varphi$. Therefore $\psi' \circ \Phi = E(\varphi') = E(\varphi) = \psi \circ \Phi$ and as Φ is an isomorphism, we conclude $\psi' = \psi$. That is ψ also is uniquely determined.

(iii) It remains to proof the equivalence for coproducts: But it is obvious, that (P, π_i) being a coproduct of the X_i in $\mathcal{C}$ is just the same, as (P, π_i) being a product of the X_i in $\mathcal{C}^{\mathrm{op}}$. And by the above, this is equivalent to $(E(P), E(\pi_i))$ being a product of the $E(X_i)$ in $\mathcal{D}^{\mathrm{op}}$. And this is just $(E(P), E(\pi_i))$ being a coproduct of the $E(X_i)$ in $\mathcal{D}$, again.

□

Proof of (11.38):

(i) Proving the uniqueness (up to isomorphy) of an object satisfying a universal property always follows the same ideas: Let us take (L, λ_i) as a direct target of the direct limit (L, λ_i). That is there is a uniquely determined morphism $\tau : L \to L$ such that $\lambda_i = \tau \circ \lambda_i$ for any $i \in I$. And clearly $\tau = \mathbb{1}_L$ does the trick. Now take (L', λ'_i) as a direct target of the direct limit (L, λ_i). Then we find a uniquely determined morphism $\lambda' : L \to L'$ such that $\lambda'_i = \lambda' \circ \lambda_i$ for any $i \in I$. Likewise let

us interchange the roles of (L,λ_i) and (L',λ'_i). That is we find a uniquely determined morphism $\lambda : L' \to L$ such that $\lambda_i = \lambda \circ \lambda'_i$ for any $i \in I$.

Let us now compose these morphisms λ' and λ: We find $(\lambda \circ \lambda') \circ \lambda_i = \lambda \circ (\lambda' \circ \lambda_i) = \lambda \circ \lambda'_i = \lambda_i$. That is $\tau = \lambda \circ \lambda'$ always satisfies $\tau \circ \lambda_i = \lambda_i$ and thereby we conclude $\lambda \circ \lambda' = \mathbb{1}_L$ as this is the only morphism, that can do the trick. In complete analogy we find $(\lambda' \circ \lambda) \circ \lambda'_i = \lambda' \circ (\lambda \circ \lambda'_i) = \lambda' \circ \lambda_i = \lambda'_i$ such that $\tau' = \lambda' \circ \lambda$ always satisfies $\tau' \circ \lambda'_i = \lambda'_i$. By the same reasoning we conclude $\lambda' \circ \lambda = \mathbb{1}_{L'}$ and thereby λ and λ' are mutually inverse. In particular $\lambda' : L \xrightarrow{\sim} L'$ is an isomorphism.

(ii) The proof follows exactly the same lines, as the proof of (i) above. We present it for completeness purposes, only: Let us take (L,λ_i) as an inverse target of the inverse limit (L,λ_i). That is there is a uniquely determined morphism $\tau : L \to L$ such that $\lambda_i = \lambda_i \circ \tau$ for any $i \in I$. And clearly $\tau = \mathbb{1}_L$ does the trick. Now take (L',λ'_i) as a direct target of the direct limit (L,λ_i). Then we find a uniquely determined morphism $\lambda' : L' \to L$ such that $\lambda'_i = \lambda_i \circ \lambda'$ for any $i \in I$. Likewise let us interchange the roles of (L,λ_i) and (L',λ'_i). That is we find a uniquely determined morphism $\lambda : L \to L'$ such that $\lambda_i = \lambda'_i \circ \lambda$ for any $i \in I$.

Let us now compose these morphisms λ' and λ: We find $\lambda_i \circ (\lambda' \circ \lambda) = (\lambda_i \circ \lambda') \circ \lambda = \lambda'_i \circ \lambda = \lambda_i$. That is $\tau = \lambda' \circ \lambda$ always satisfies $\lambda_i \circ \tau = \lambda_i$ and thereby we conclude $\lambda' \circ \lambda = \mathbb{1}_L$ as this is the only morphism, that can do the trick. In complete analogy we find $\lambda'_i \circ (\lambda \circ \lambda') = (\lambda'_i \circ \lambda) \circ \lambda' = \lambda_i \circ \lambda' = \lambda'_i$ such that $\tau' = \lambda \circ \lambda'$ always satisfies $\lambda'_i \circ \tau' = \lambda'_i$. By the same reasoning we conclude $\lambda \circ \lambda' = \mathbb{1}_{L'}$ and thereby λ and λ' are mutually inverse. In particular $\lambda : L \xrightarrow{\sim} L'$ is an isomorphism.

(iii) Let us first prove (b) $\Longrightarrow$ (a) for direct limits: That is for any direct target (T,τ_i) we need to find a uniquely determined morphism $\tau : L \to T$ such that $\tau \circ \lambda_i = \tau_i$ for any $i \in I$. Let us shift the whole (left-hand) diagram in (11.37) under E. By assumption (b) there is a uniquely determined morphism $\vartheta : E(L) \to E(T)$ such that $\vartheta \circ E(\lambda_i) = E(\tau_i)$ for any $i \in I$. By (11.31.(ii)) E is full and faithful. Hence there is a uniquely determined morphism $\tau : L \to T$ such that $E(\tau) = \vartheta$ and therefore

$$E\big(\tau \circ \lambda_i\big) \;=\; E(\tau) \circ E(\lambda_i) \;=\; \vartheta \circ E(\lambda_i) \;=\; E(\tau_i)$$

such that $\tau \circ \lambda_i = \tau_i$ by faithfulness. That is τ satisfies the properties required. It remains to veritfy its uniqueness: That is we consider any $\tau' : L \to T$ such that $\tau' \circ \lambda_i = \tau_i$. Then we get

$$E(\tau') \circ E(\lambda_i) \;=\; E\big(\tau' \circ \lambda_i\big) \;=\; E(\tau_i) \;=\; \vartheta \circ E(\lambda_i)$$

As this is true for any $i \in I$ we find $E(\tau') = \vartheta = E(\tau)$, as ϑ is unique with this property, and thereby $\tau' = \tau$ by faithfulness, again. Thus τ also is uniquely determined.

(iii) Conversely for (a) $\Longrightarrow$ (b) for direct limits: We have to prove that $(E(L), E(\lambda_i))$ is a direct limit, that is for any direct target (T,τ_i) we need to find some $\tau : E(L) \to T$ such that for any $i \in I$ we have $\tau \circ E(\lambda_i) = \tau_i$. And this τ has to be uniquely determined, by this property. By (11.31.(ii)) E not only is full and faithful, but also essentially surjective. That is we can choose some $S \in \mathrm{obj}(\mathcal{C})$ such that $\Phi : T \xrightarrow{\sim} E(S)$ admits an isomorphism Φ. Then we have $\Phi \circ \tau_i : E(M_i) \to E(S)$ and hence there is a uniquely determined morphism $\sigma_i : M_i \to S$ such that $E(\sigma_i) = \Phi \circ \tau_i$. By assumption

(T, τ_i) is a direct target of $(E(M_i), E(\mu_i^j))$ and therefore $\tau_i = \tau_j \circ E(\mu_i^j)$ for any $i \leq j \in I$. Apply Φ from the left, then we get

$$E(\sigma_i) \;=\; \Phi \circ \tau_i \;=\; \Phi \circ \tau_j \circ E(\mu_i^j) \;=\; E(\sigma_j) \circ E(\mu_i^j) \;=\; E(\sigma_j \circ \mu_i^j)$$

By faithfulness of E that is $\sigma_i = \sigma_j \circ \mu_i^j$ and this means that (S, σ_i) is a direct target of (M_i, μ_i^j). Therefore, by assumption (a), there is a uniquely determined morphism $\sigma : L \to S$, such that $\sigma \circ \lambda_i = \sigma_i$ for any $i \in I$. Take $\tau := \Phi^{-1} \circ E(\sigma) : E(L) \to T$, then we get

$$\tau \circ E(\lambda_i) \;=\; \Phi^{-1} \circ E(\sigma) \circ E(\lambda_i) \;=\; \Phi^{-1} \circ E(\sigma \circ \lambda_i) \;=\; \Phi^{-1} \circ E(\sigma_i) \;=\; \Phi^{-1} \circ \Phi \circ \tau_i \;=\; \tau_i$$

That is τ satisfies the properties required for a direct limit. It remains to verify the uniqueness: Suppose we had another morphism $\tau' : E(L) \to T$ such that for any $i \in I$ we get $\tau' \circ E(\lambda_i) = \tau_i$. Then $\Phi \circ \tau' : E(L) \to E(S)$ and thereby there is a (uniquely determined) $\sigma' : L \to S$, such that $E(\sigma') = \Phi \circ \tau'$. Then we find

$$E(\sigma' \circ \lambda_i) \;=\; E(\sigma') \circ E(\lambda_i) \;=\; \Phi \circ \tau' \circ E(\lambda_i) \;=\; \Phi \circ \tau_i \;=\; E(\sigma_i)$$

By faithfulness of E this is $\sigma' \circ \lambda_i = \sigma_i$ again, and as this is true for any $i \in I$ and σ is unique with this property, we conclude $\sigma' = \sigma$. In particular $\Phi \circ \tau' = E(\sigma') = E(\sigma) = \Phi \circ \tau$. And as Φ is an isomorphism we may apply Φ^{-1} from the left to find $\tau' = \tau$ which also is the uniqueness of τ.

(iii) It remains to proof the equivalence for inverse limits: But it is obvious, that (L, λ_i) being an inverse limit of (M_i, μ_j^i) in $\mathcal{C}$ is just the same, as (L, λ_i) being a direct limit of (M_i, μ_j^i) in $\mathcal{C}^{\mathrm{op}}$. And by the above, this is equivalent to $(E(L), E(\lambda_i))$ being a direct limit of $(E(M_i), E(\mu_j^i))$ in $\mathcal{D}^{\mathrm{op}}$. And this is just $(E(P), E(\lambda_i))$ being an inverse limit of $(E(M_i), E(\mu_j^i))$ in $\mathcal{D}$, again.

□